Strong authentication for Cisco ASA 5500 Clientless SSL VPN and Cisco VPN Client Solutions with

nordic edge

One Time Password Server

The complete installation guide for securing the authentication to your Cisco ASA 5500 solution with Nordic Edge One Time Password Server, delivering two-factor authentication via SMS to your mobile phone. For both clientless SSL VPN and Cisco VPN Client.

Content

1 Summary

This is the complete installation guide for securing the authentication to your Cisco ASA 5500 solution with Nordic Edge One Time Password Server, delivering two-factor authentication via SMS to your mobile phone. For both clientless SSL VPN and Cisco VPN Client. You will be able to test the product with your existing Cisco ASA 500 and LDAP user database, without making any changes that affect existing users. The guide will also allow you to make the complete installation effeciently, using a maximum of 1 hour. Nordic Edge provides several methods for delivering one time passwords, like e-mail, tokens, mobile clients, prefetch etc. - however in this test we are only going to use SMS.

This is a step-by-step guide that covers the entire installation from A to Z. It is based on the scenario that you are running your Cisco 5500 solution against Active Directory, and that you install the One Time Password Server on a Windows Server. The One Time Password Server is platform independent and works with all other LDAP user databases, like eDirectory, Sun One, Open LDAP etc. If you are not running Active Directory or Windows and if you have any questions regarding the slight differences in the installation process, you are most welcome to contact us at support@nordicedge.se and we will take you through the entire process.

2 Prerequisites

You will need to have a server available, for example a VMware virtual machine with Windows Server 2003 installed with Ethernet in bridge mode. The server needs to have an ip-address configured and must also be able to reach your DNS-servers, your Cisco 5500 ASA solution and the Active Directory. Since the software is quite small and easy to remove, you can also use any existing server in your network.

3 Important information regarding communication

The One Time Password Server is a software that you can place on any server in your internal network or DMZ.

- The One Time Password Server needs to be able to communicate (Outbound traffic) with your **LDAP** or **JDBC** User Database. Default port for LDAP and Secure LDAP is TCP port 389 / 636.

- The Integration Module needs to be able to communicate (Outbound traffic) with the One Time Password Server on TCP port 3100. Or Radius with UDP port 1812 or 1645 (Outbound traffic)

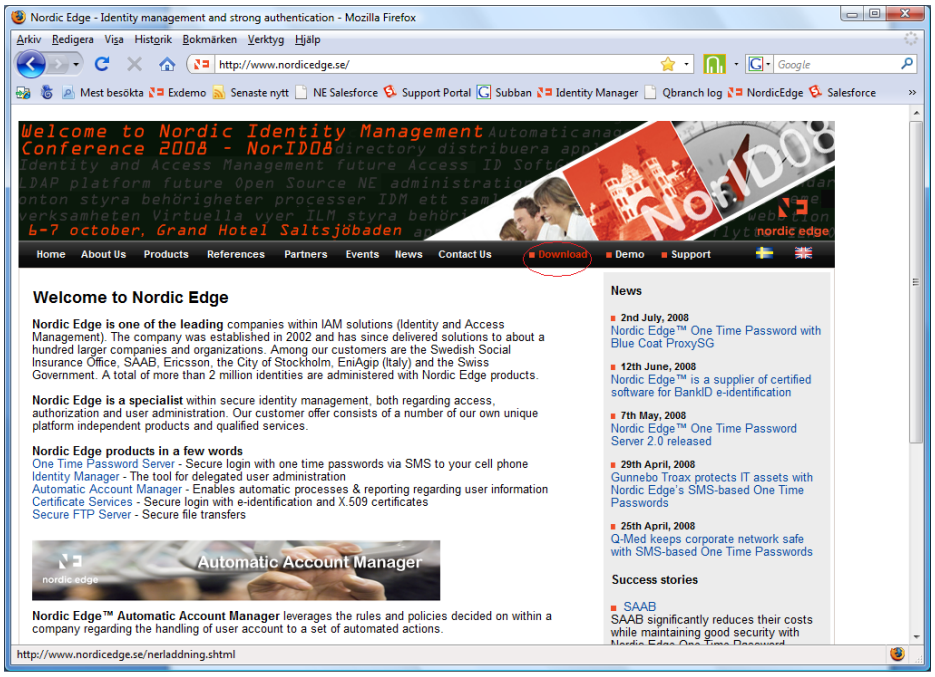
- If you want to use the **Nordic Edge SMS Gateway**, the One Time Password Server needs to be able to communicate (Outbound traffic) with otp.nordicedge.net and otp.nordicedge.se with HTTPS on TCP port 443.

In this test-scenario you will want to communicate with RADIUS port 1812 or 1645 and use our Nordic Edge SMS Gateway.

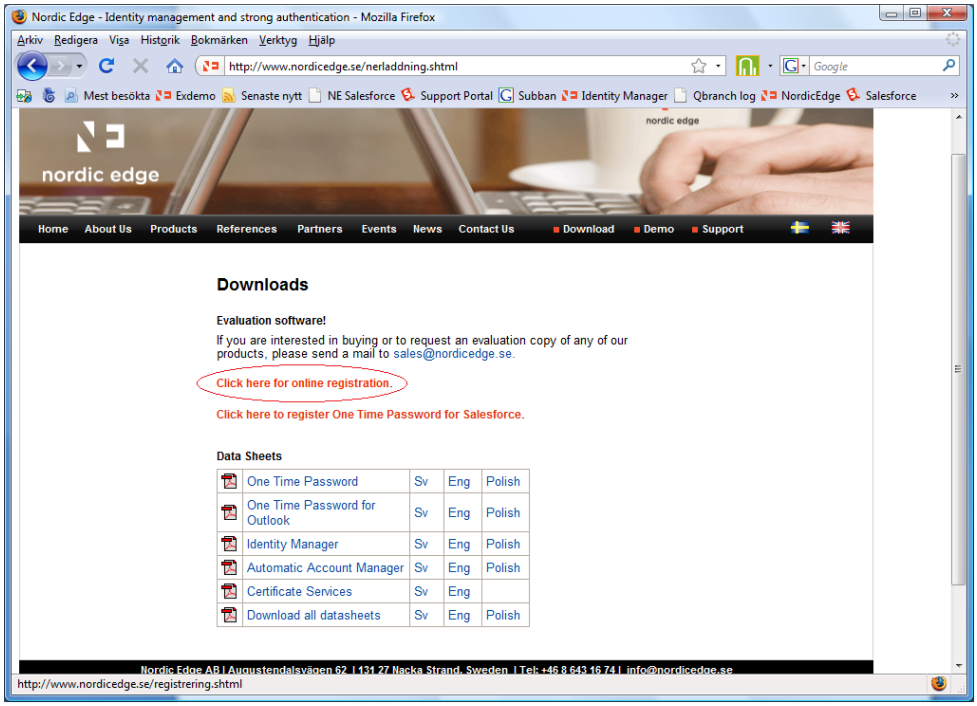
4 Getting started

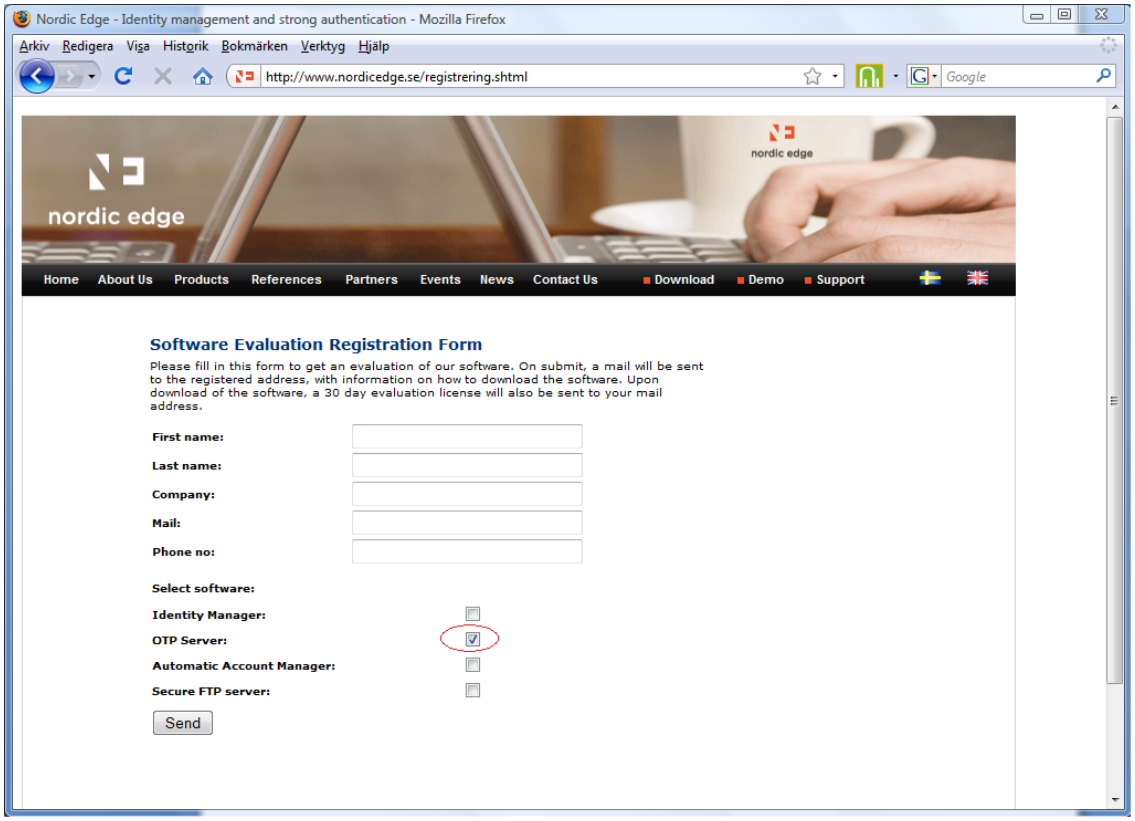
4.1 1.1 Download the software

Go to www.nordicedge.se and click on Download



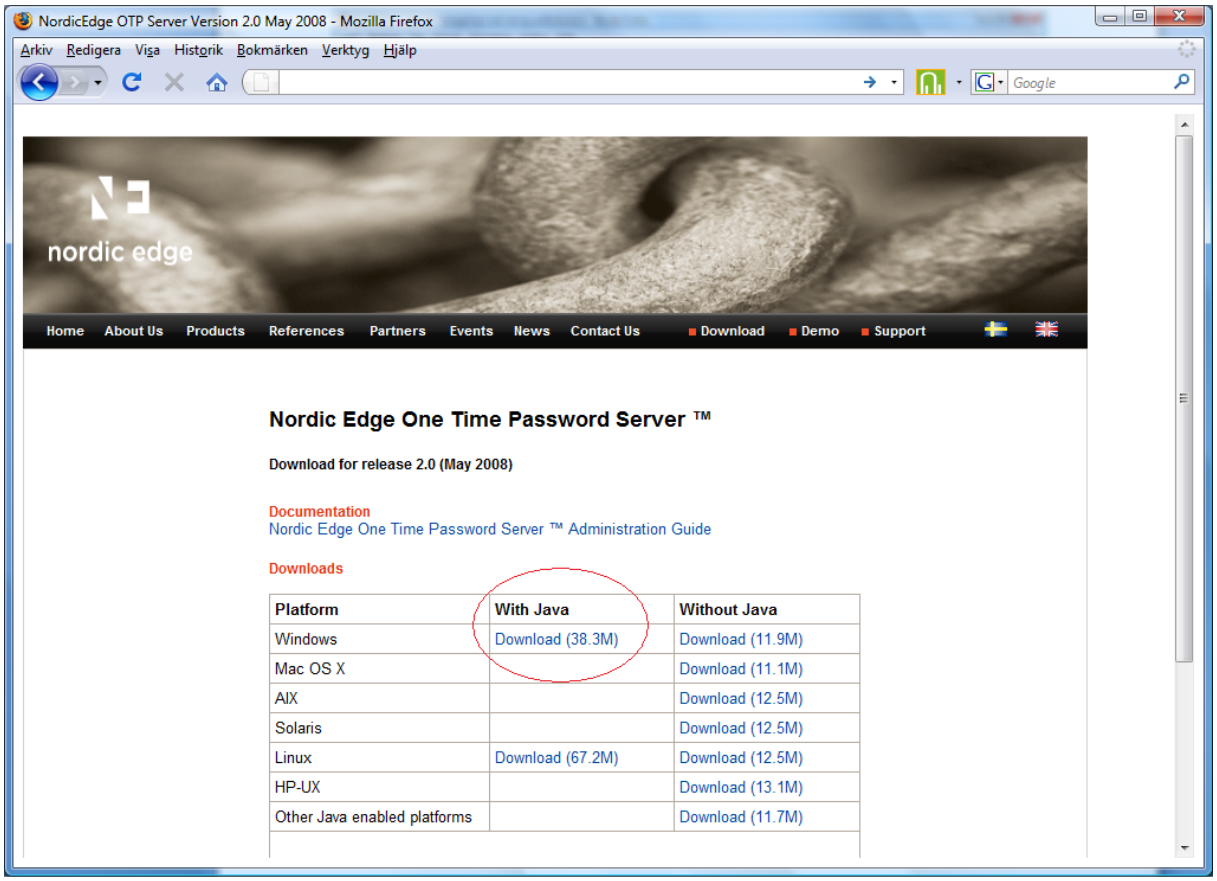
4.2 Register and download the software

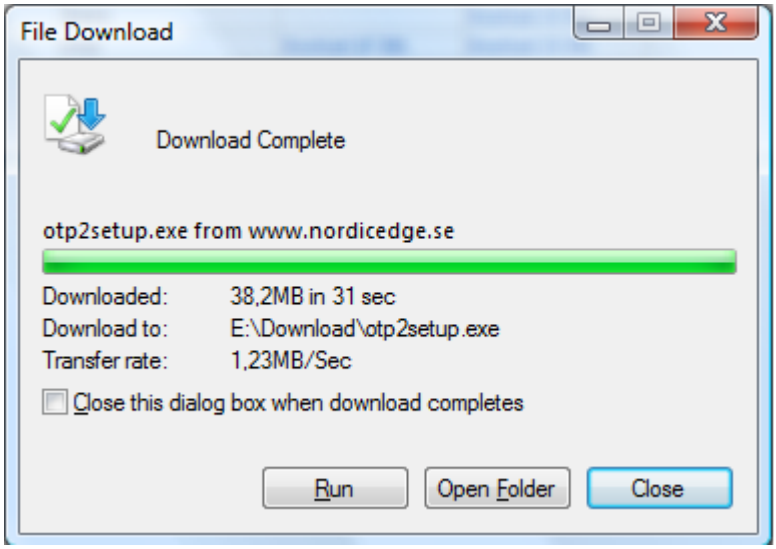




You will receive a link for downloading the software. A 30 days evaluation license will be sent via e-mail when you download the software.

Download the version with JAVA included.

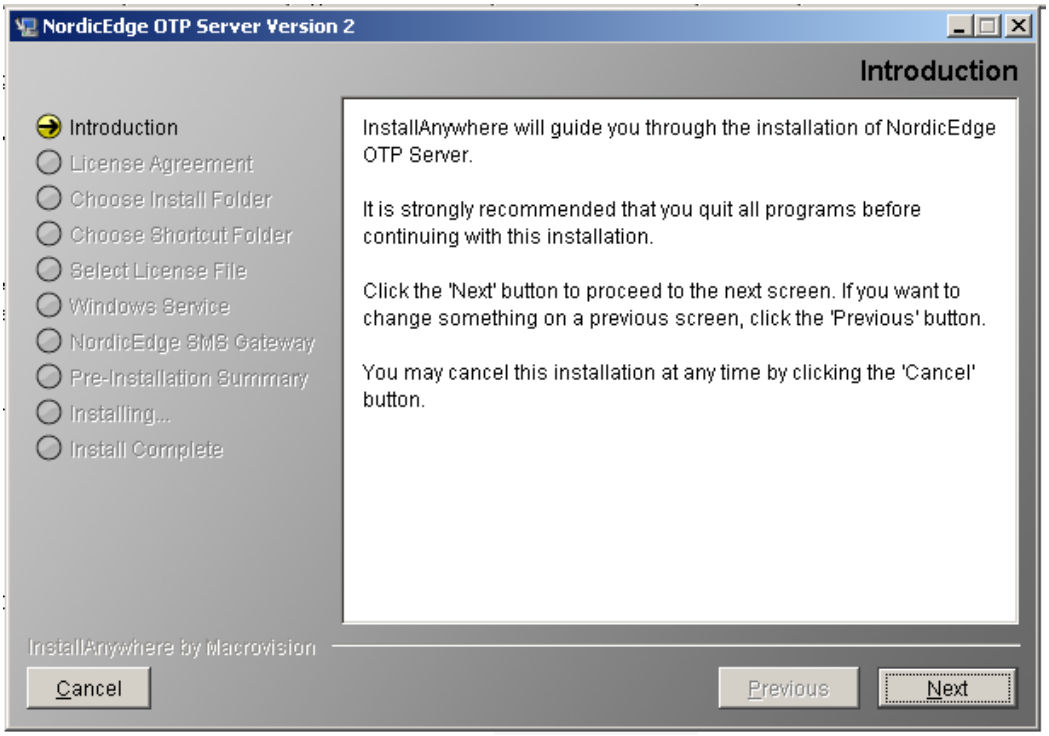


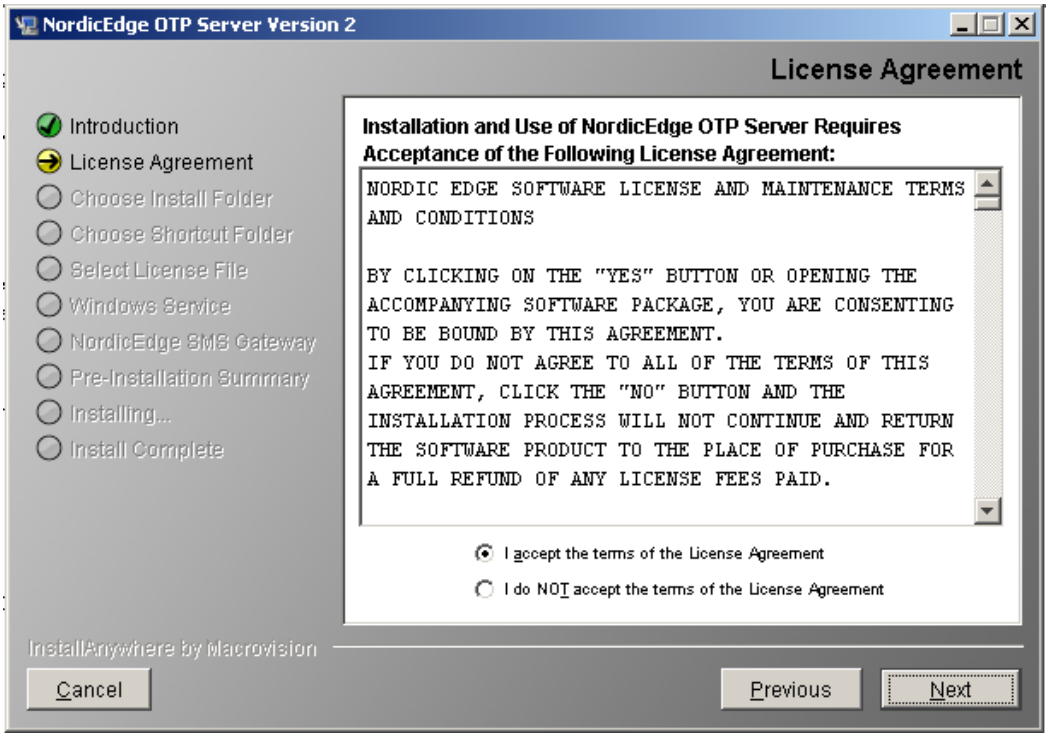


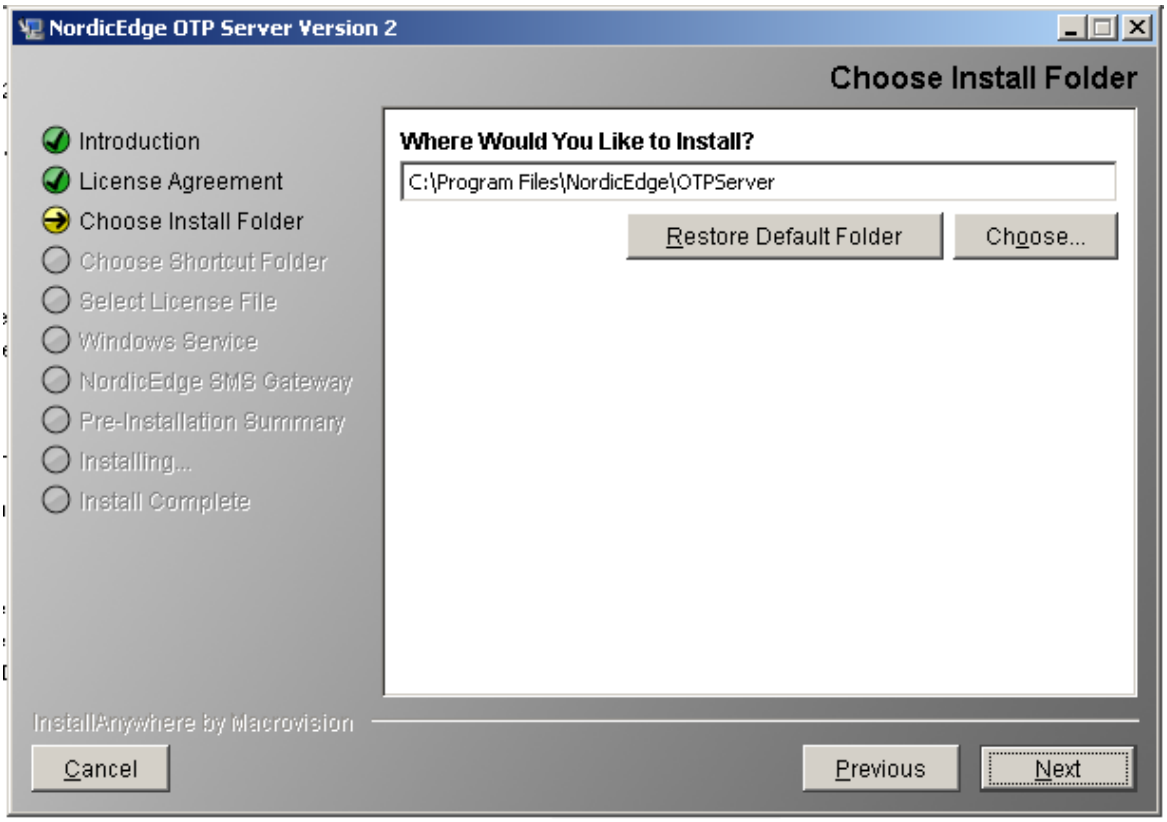
5 Installation

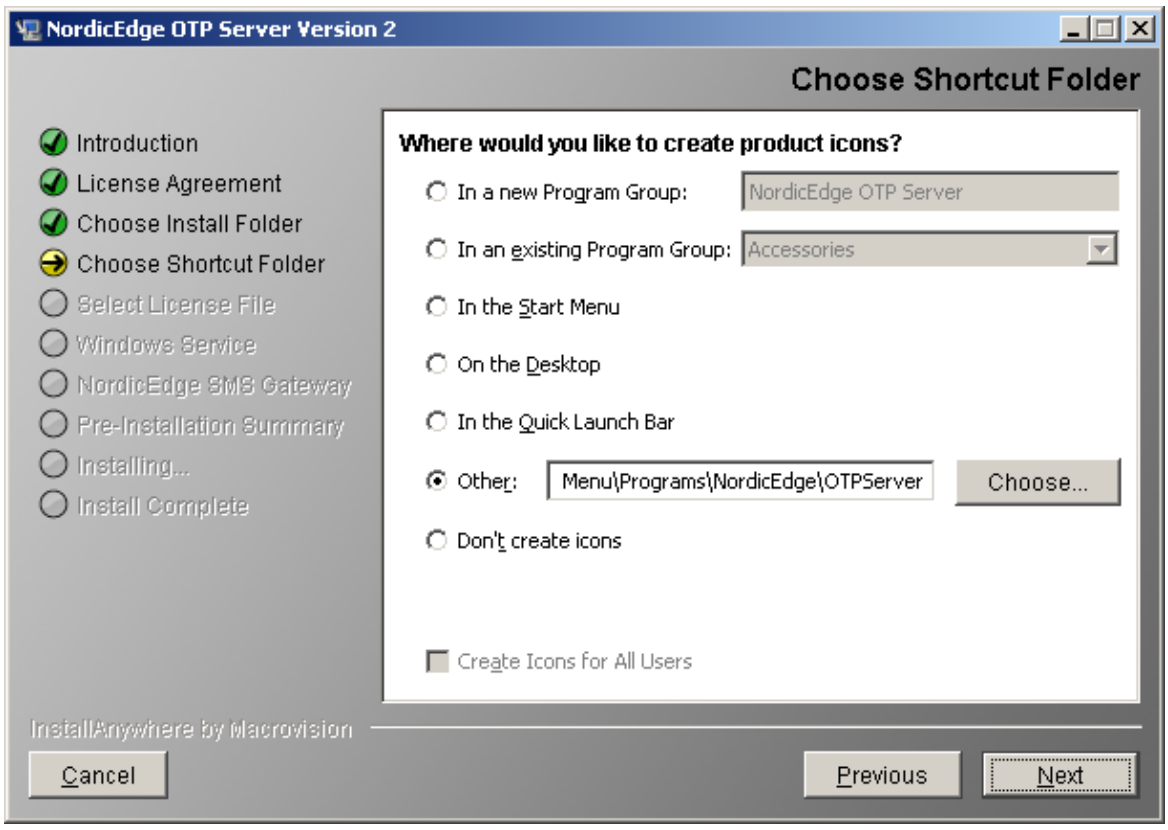
5.1 Start the installation

Start the installation on the server where you want to install the One Time Password Server



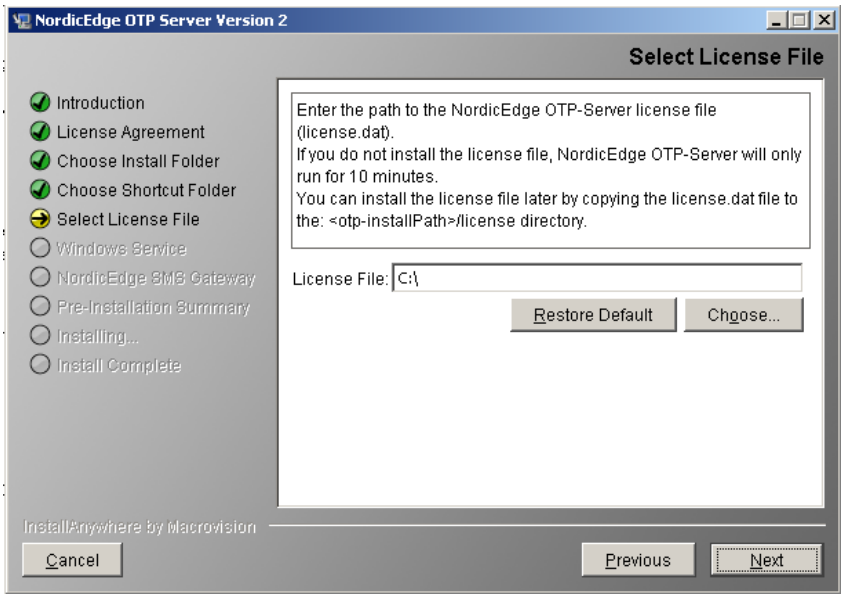


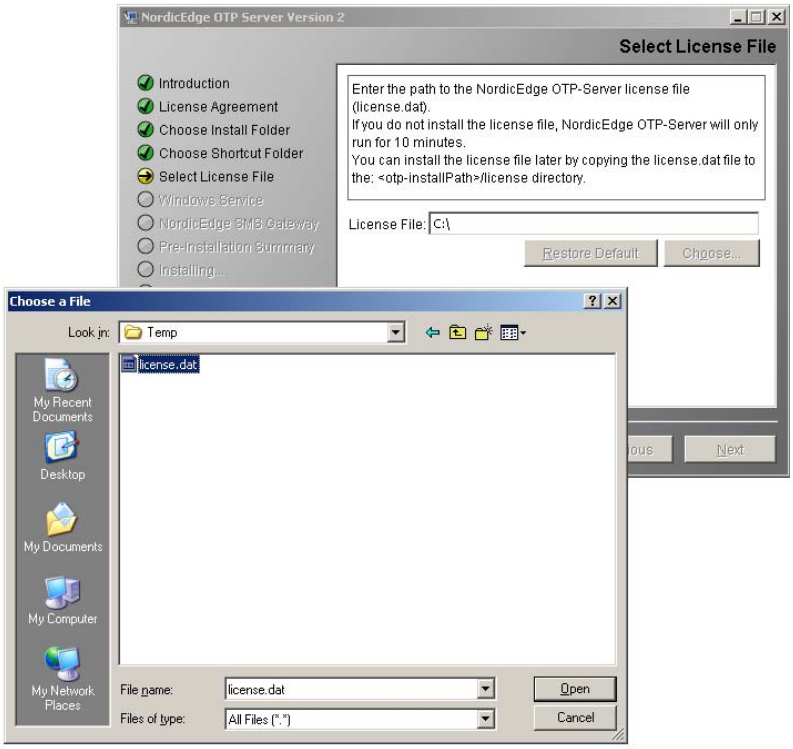


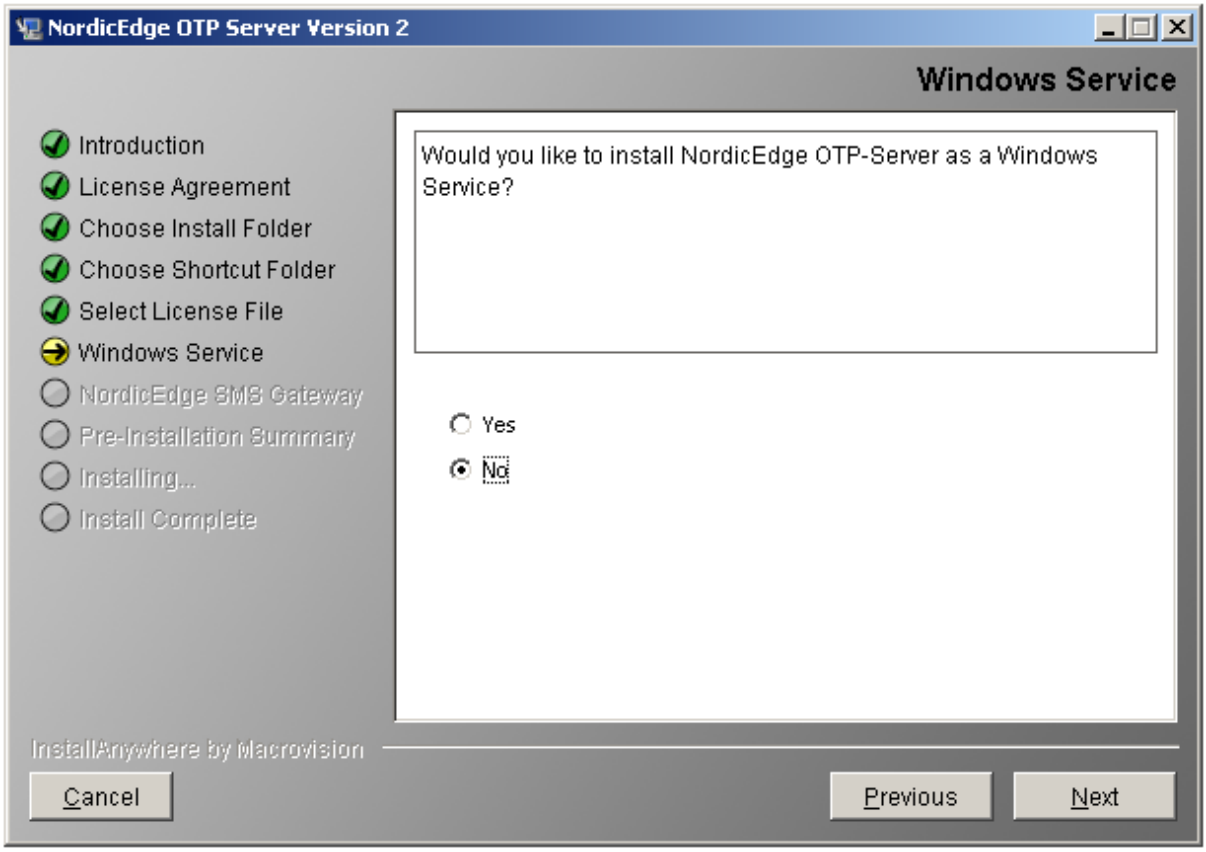


5.2 Installing license

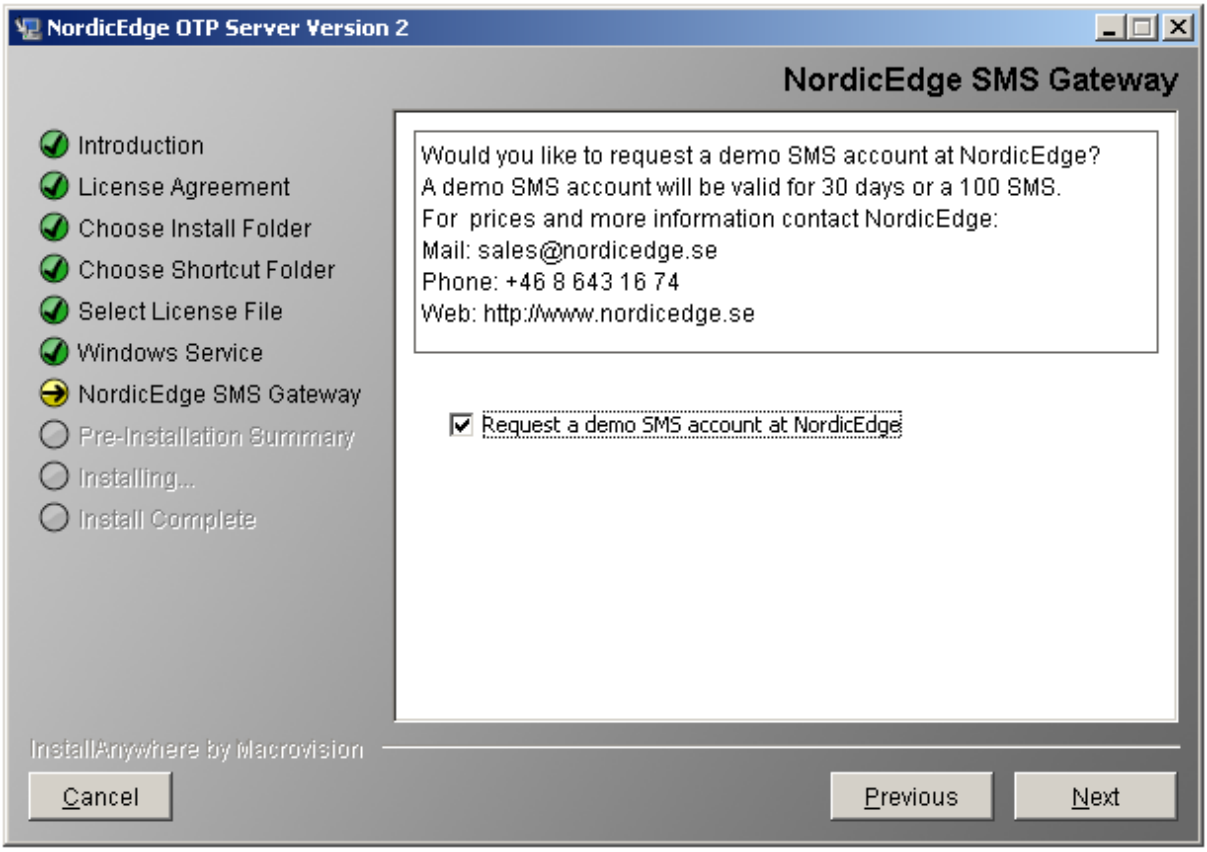
Choose the license.dat that you have received via e-mail. This is important, since if you want to request a demo SMS account at Nordic Edge later in the installation, you need to install the license at this moment.

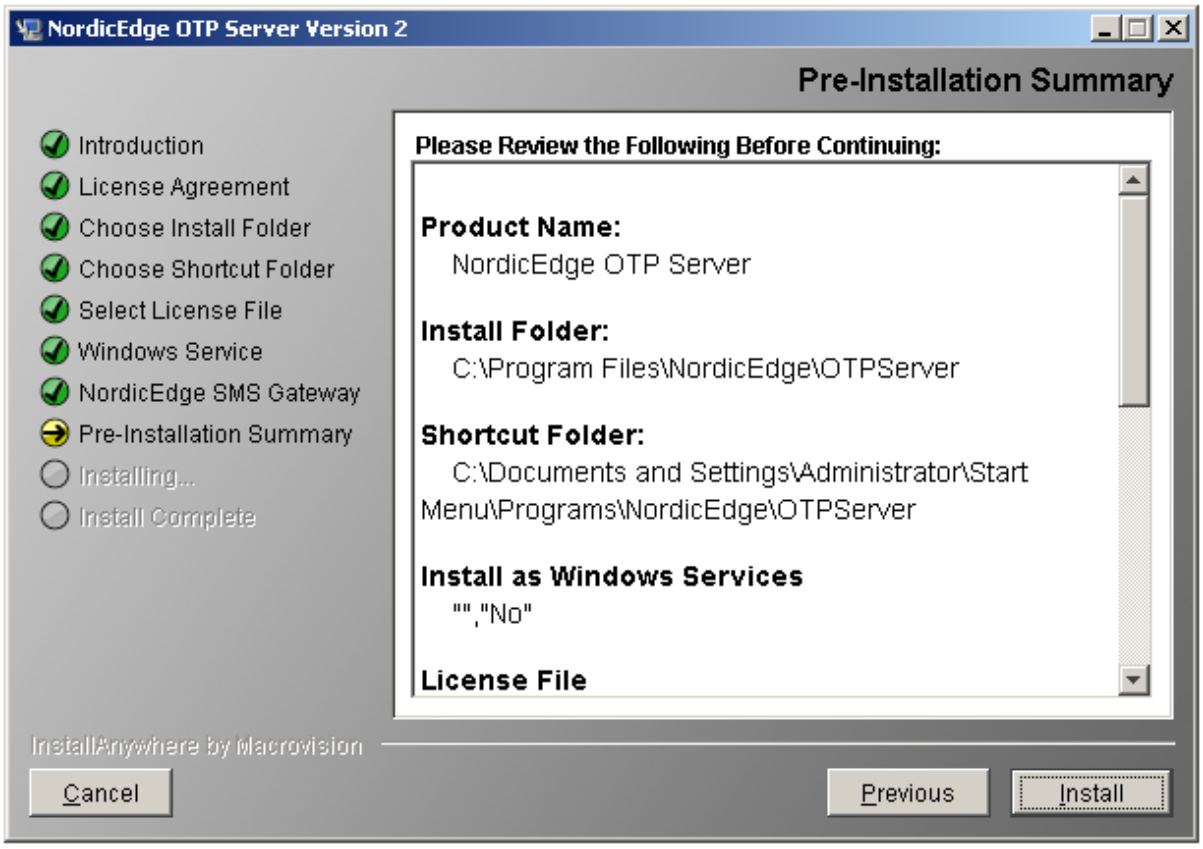


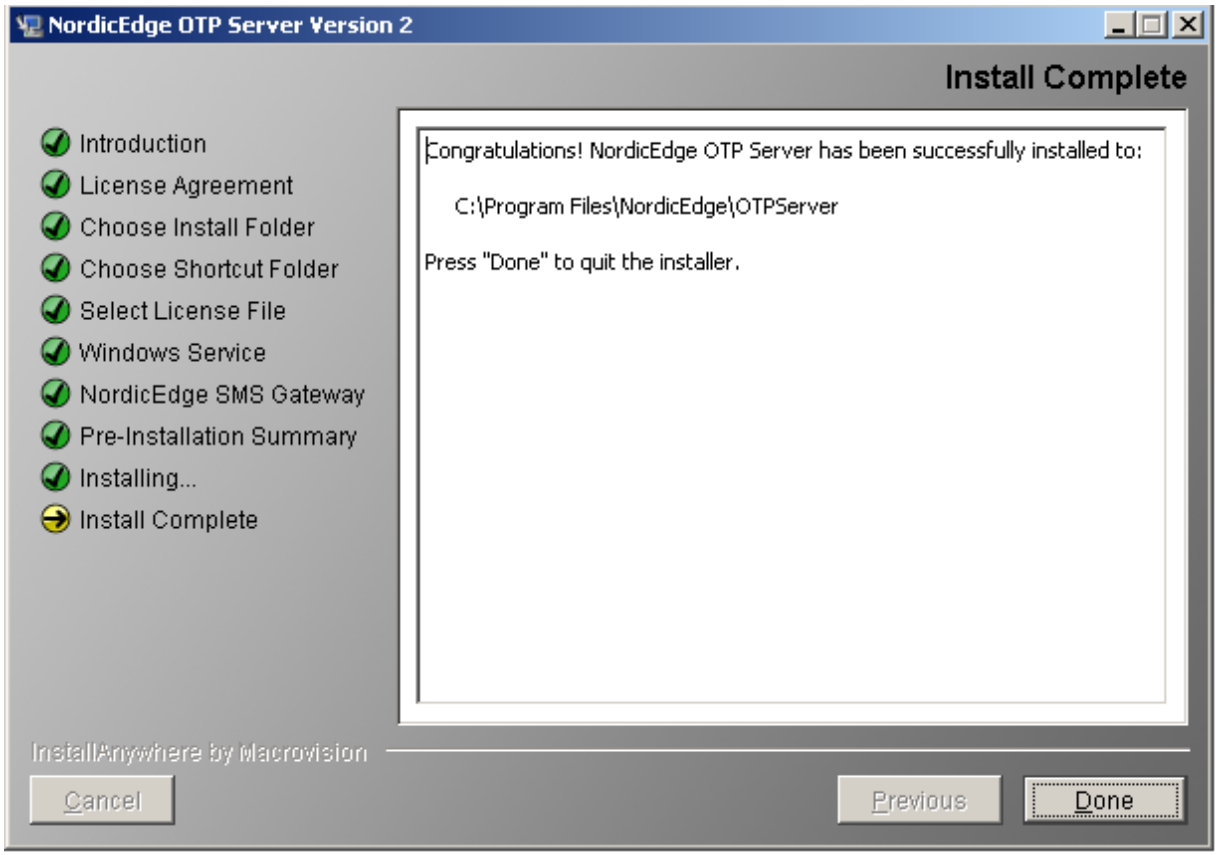




Note, if you are in a test-phase, we recommend that you do not install the OTP-Server as a Windows Service.



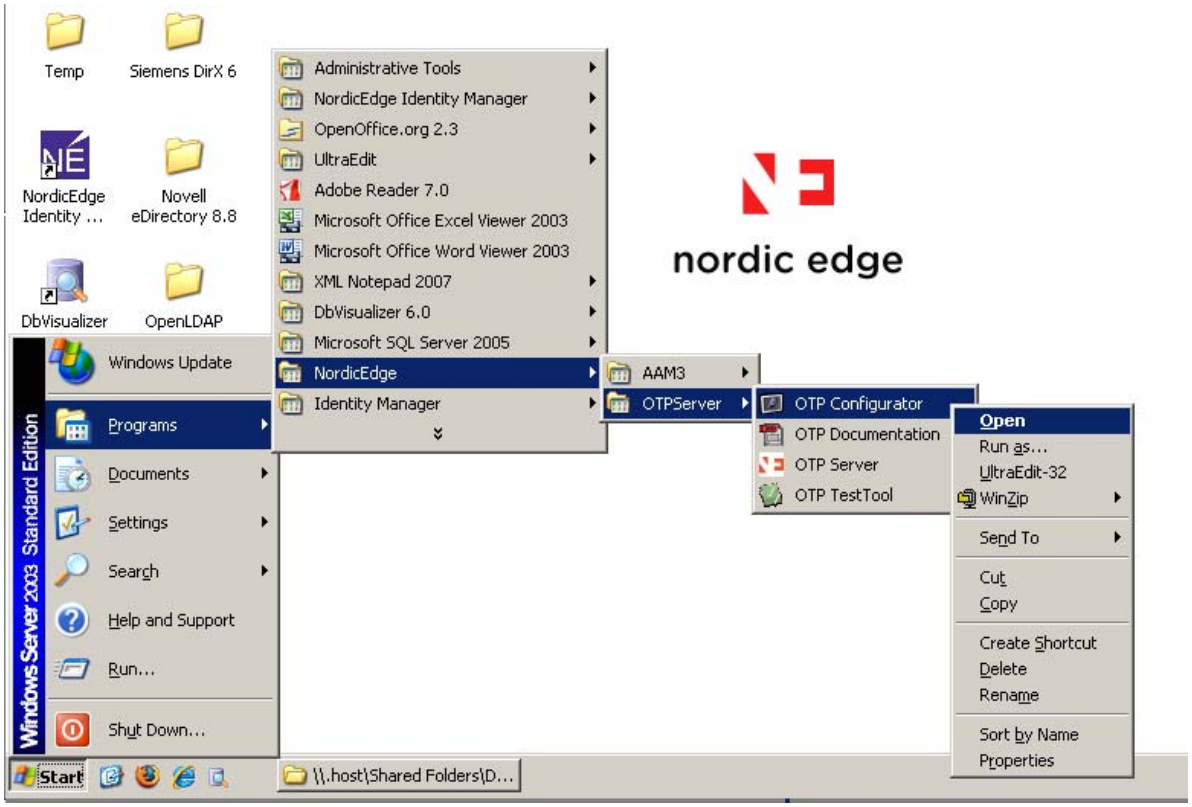




6 Configuring the One Time Password Server

6.1 Start the OTP Configuration

Start the OTP Configurator by clicking on Programs / NordicEdge / OTP Configurator

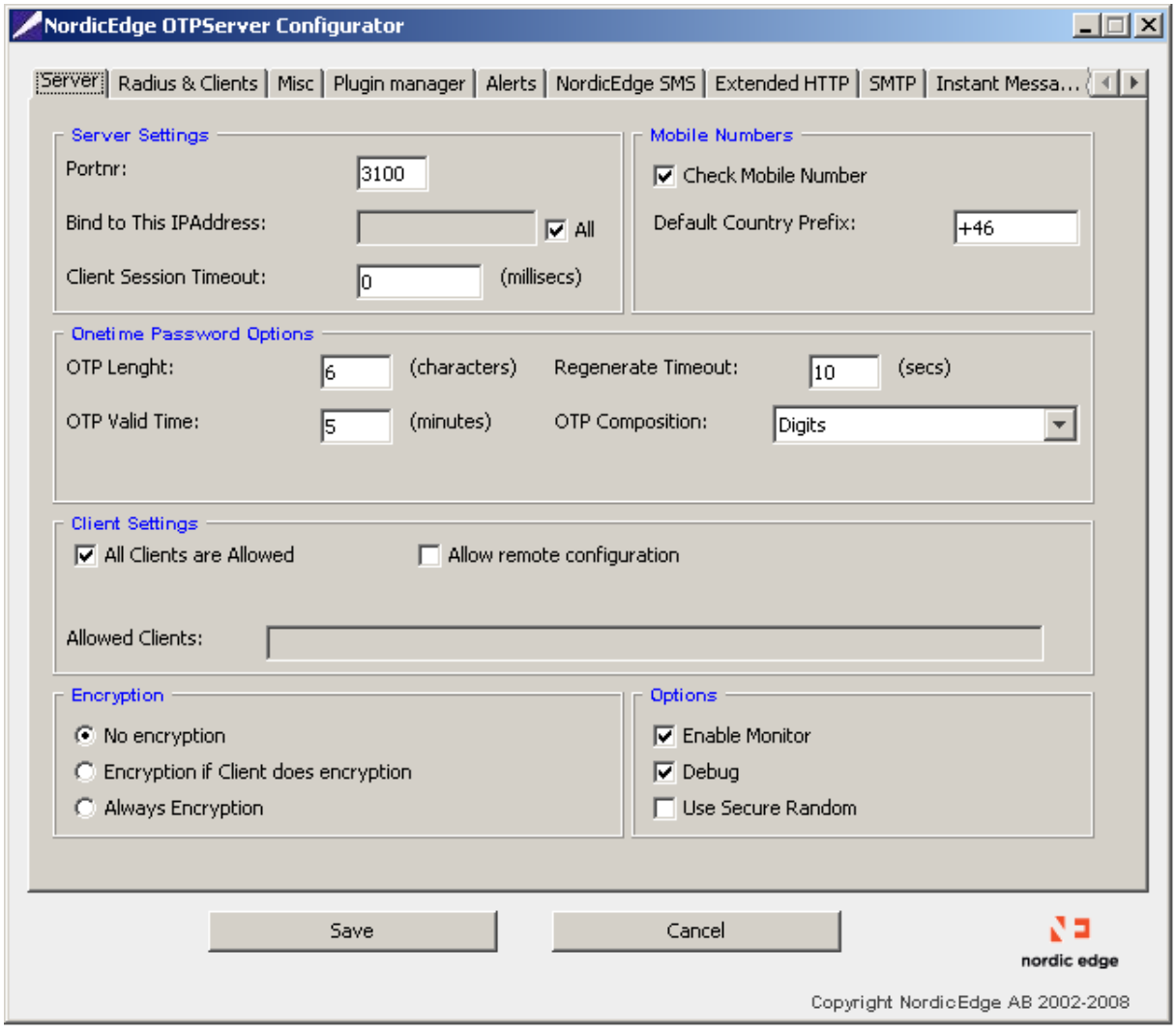


6.2 Server page

On the Server page you can set the length of the one-time password and for how long it should be valid. Default is 5 minutes.

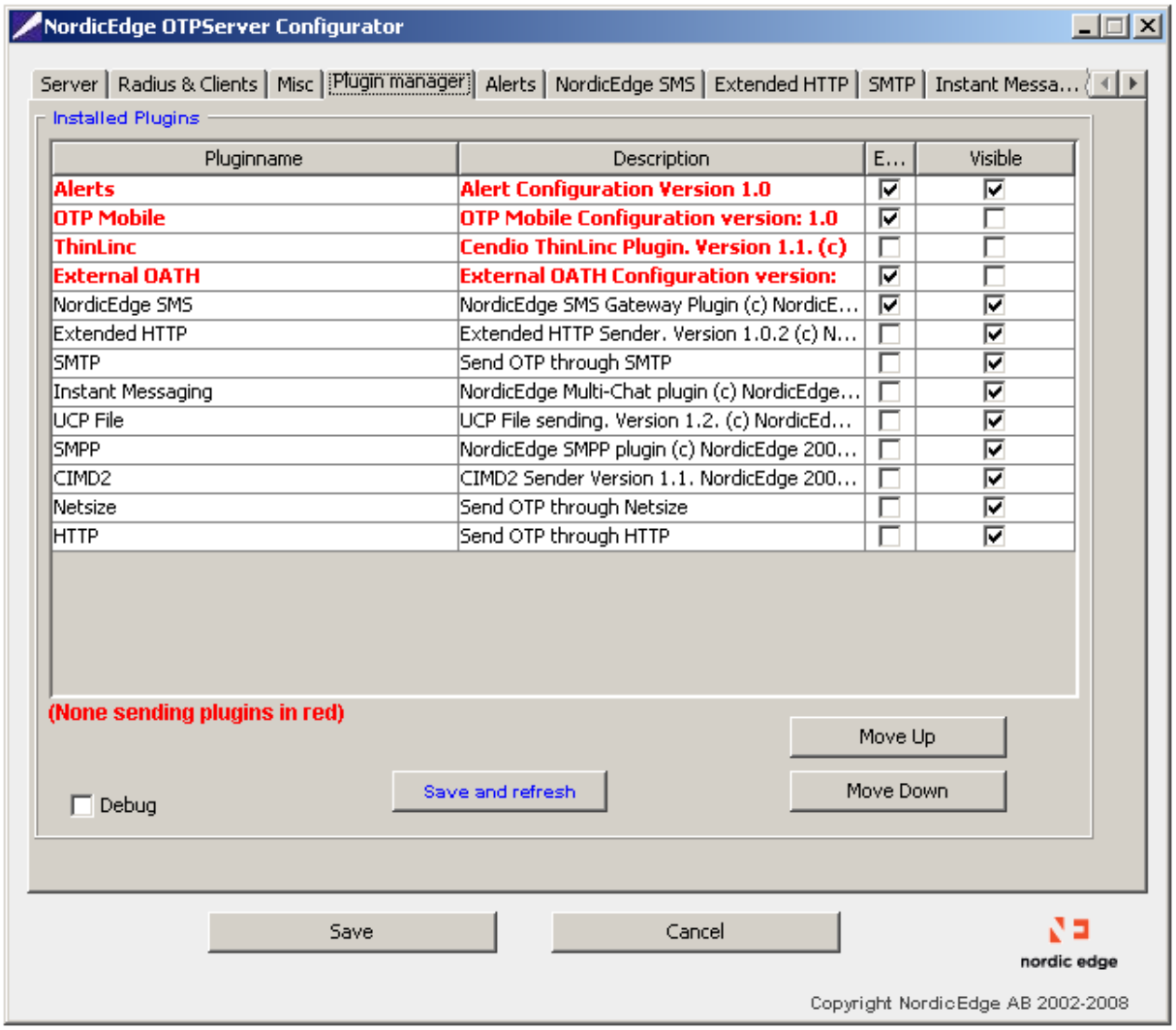
You can also set a default country prefix, which means that you will not need to state it in the mobile attribute.

The One Time Password communicates with TCP protocol portnr 3100.



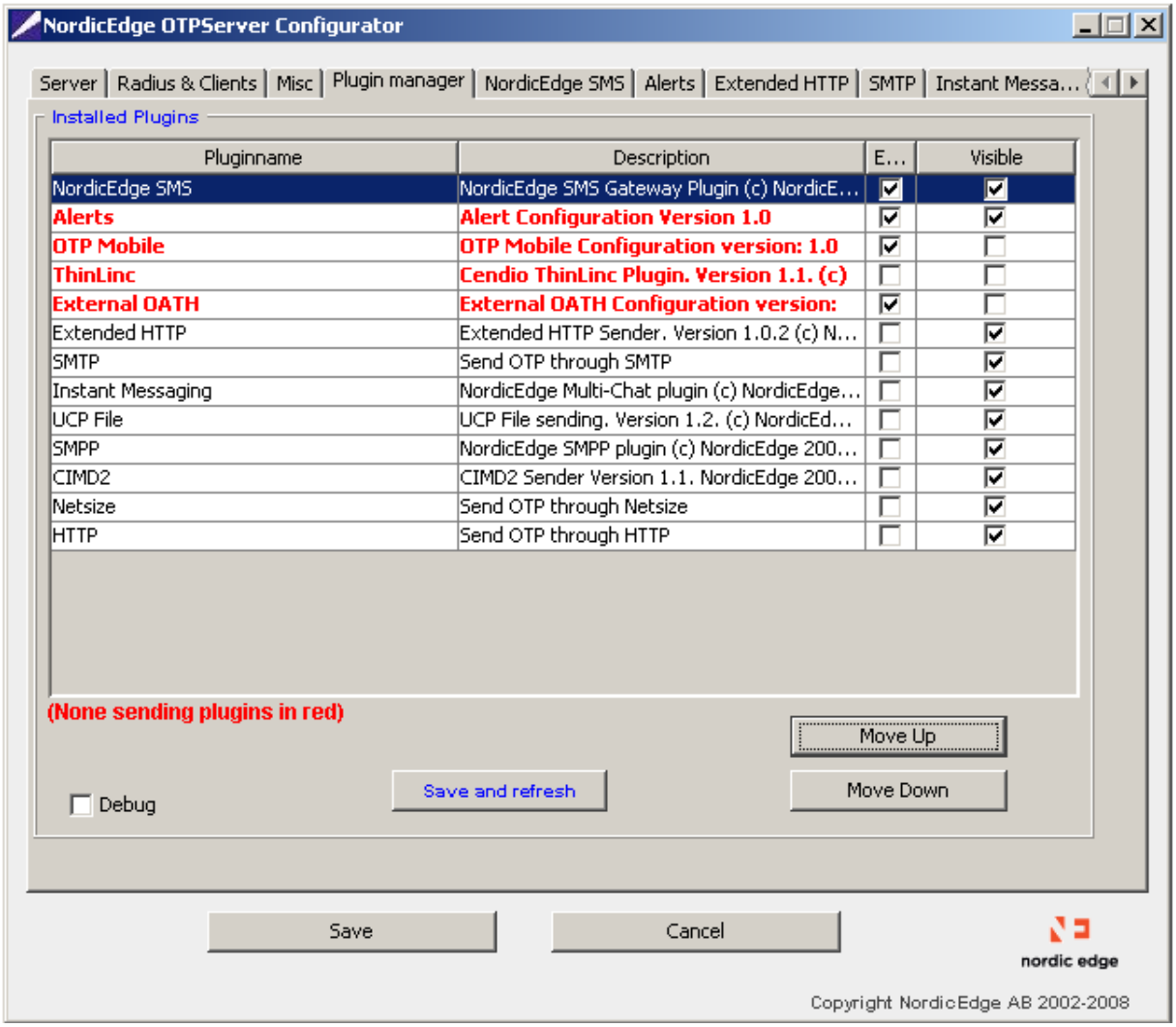
6.3 Plugin manager page

On the Plugin manager page you can configure all methods and in which order you want to use them. In this case we will be using Nordic Edge SMS gateway to deliver the one-time password via SMS to your mobile phone.



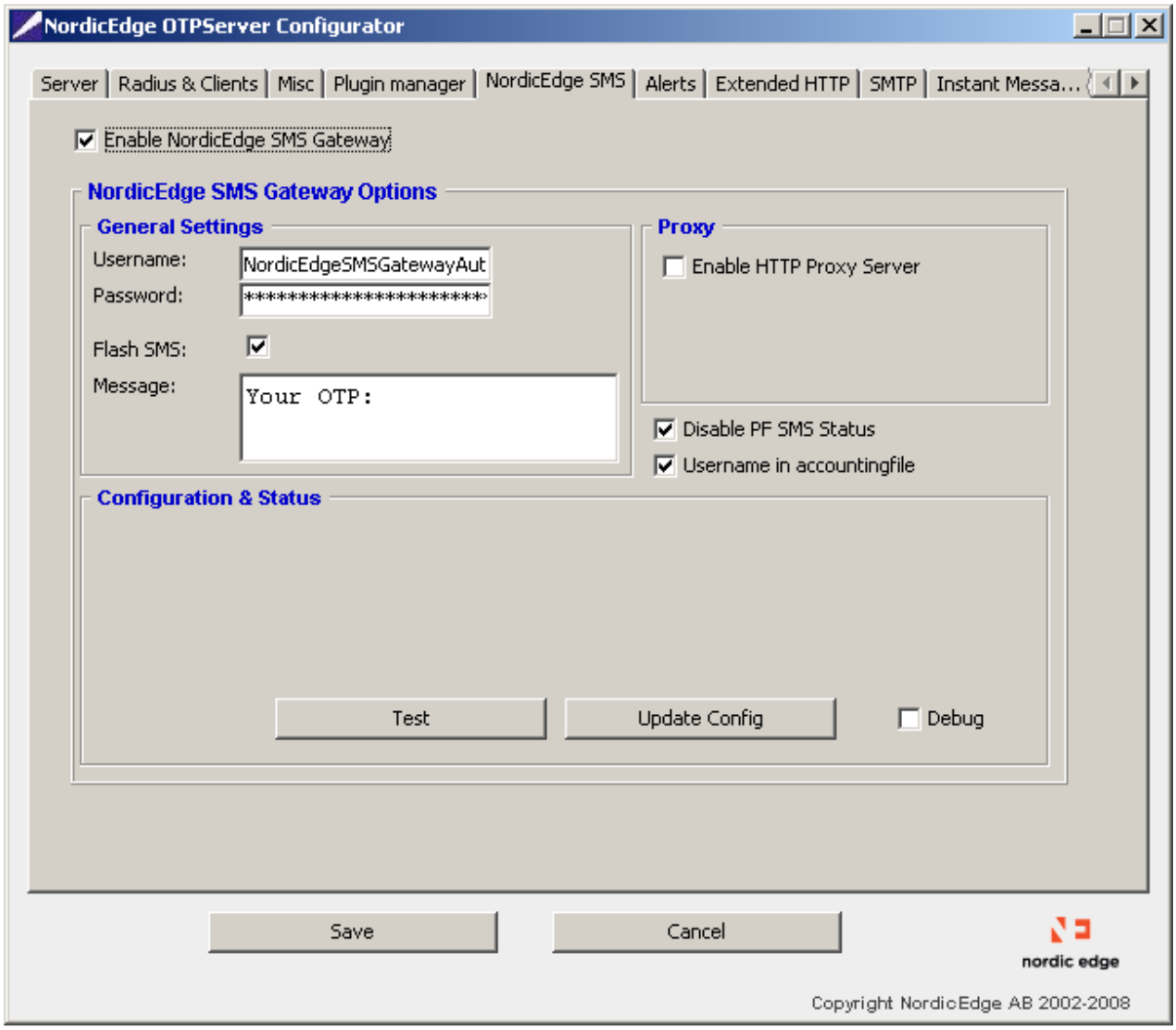
6.3.1 Nordic Edge SMS Plugin

Move the Plugin Nordic Edge SMS to the top of the plugins.



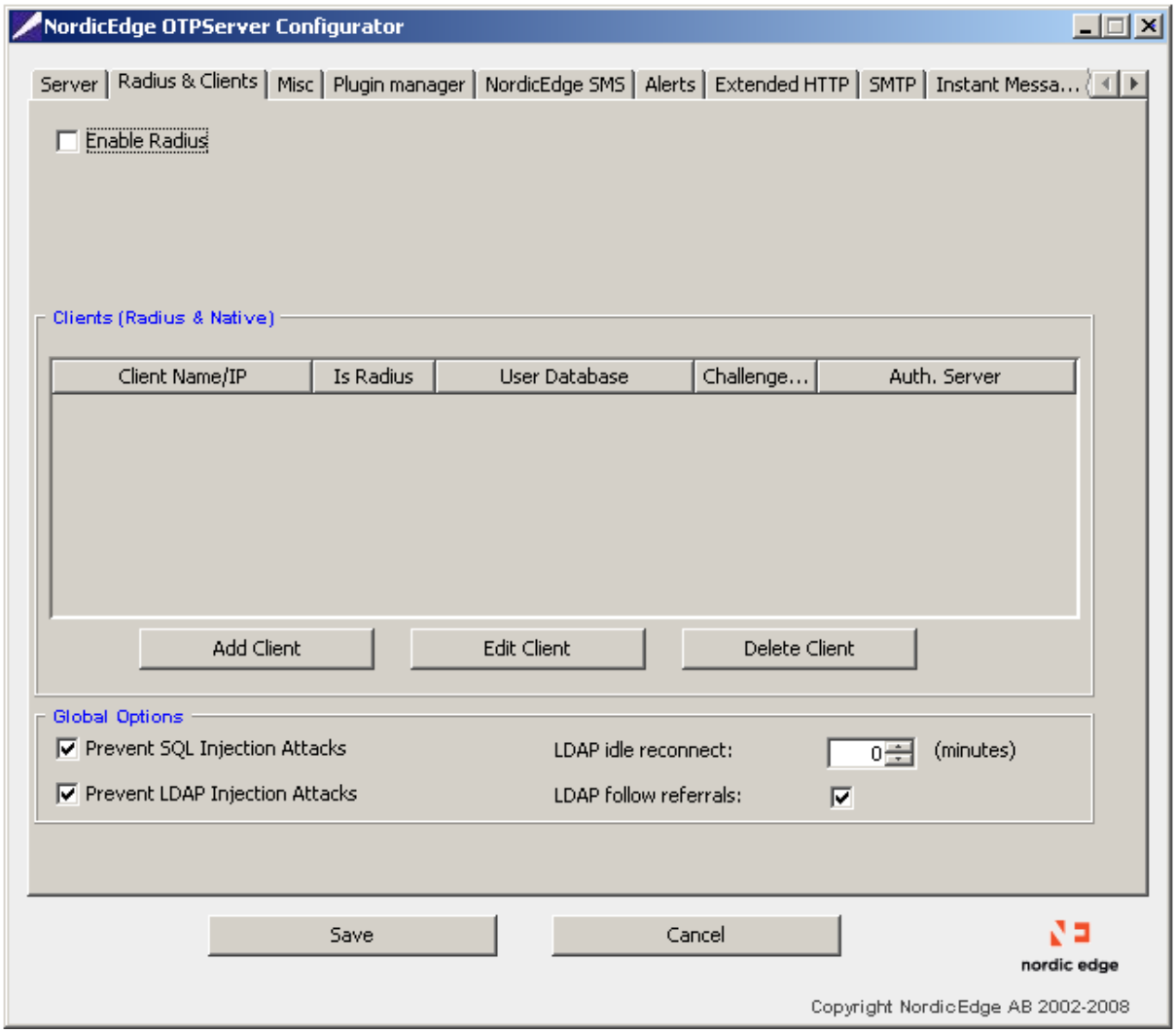
6.4 Nordic Edge SMS Page

Look at the Nordic Edge SMS Page. If you installed the license.dat during the installation and checked the box "Request a demo SMS account at Nordic Edge", an account should now be preconfigured for you.



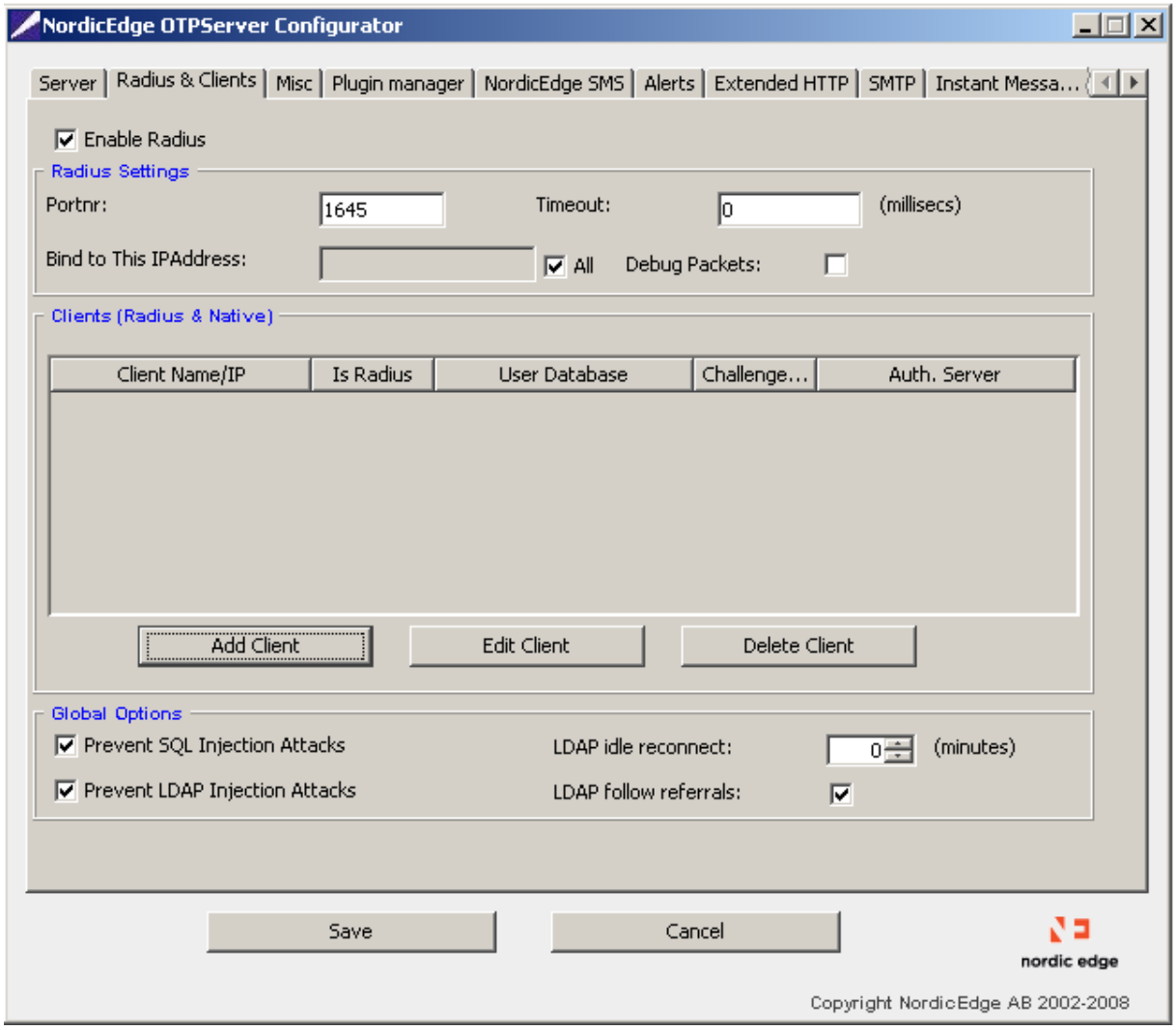
6.5 Radius & Client page

For configuring One Time Passwords Server to act as radius server go to the Radius & Client page.



6.5.1 Enable Radius

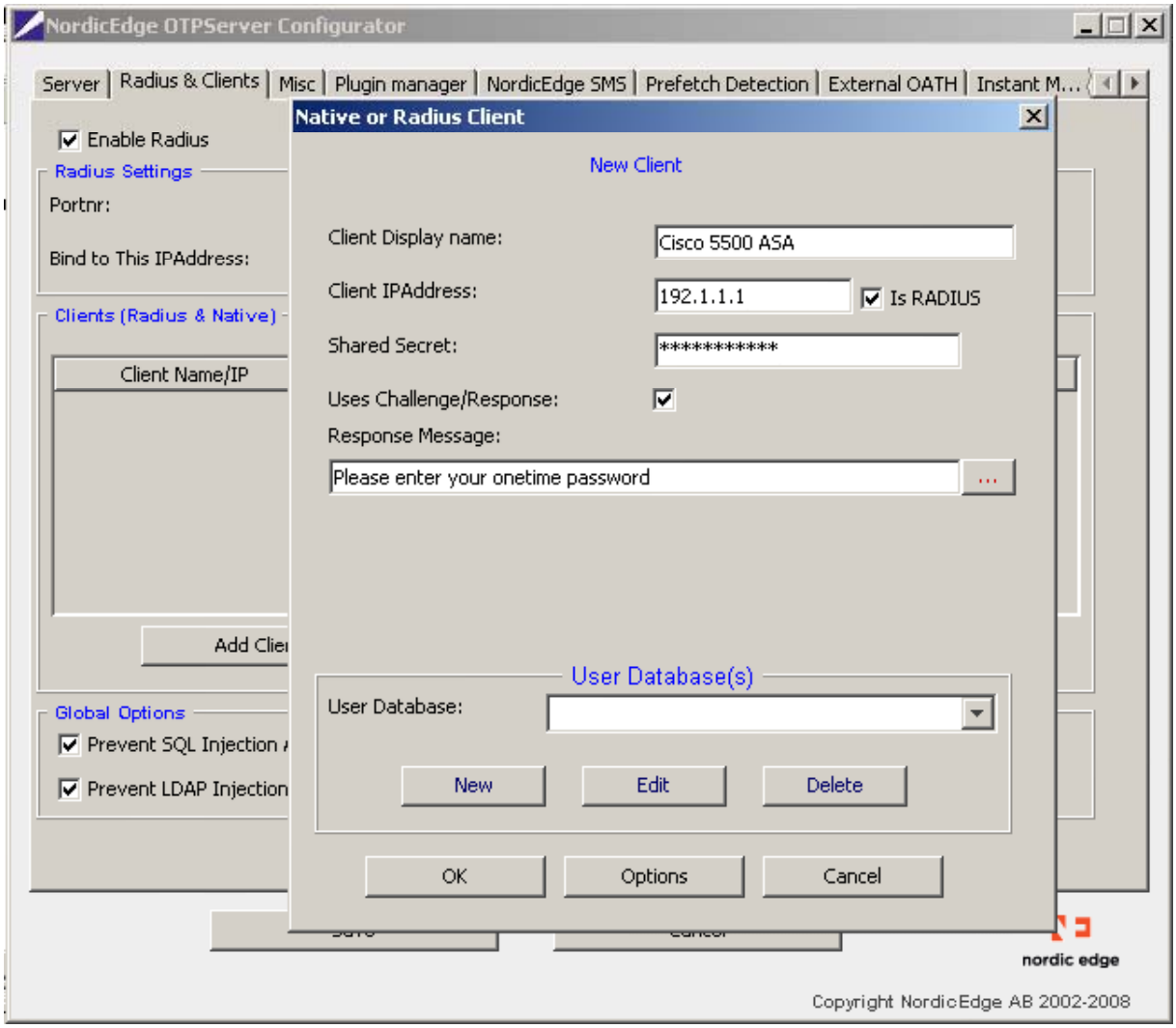
Enable Radius and choose one of the radius ports 1645 or 1812 that you want to use. Make sure that the client (Cisco 5500 ASA) is using the same radius port.



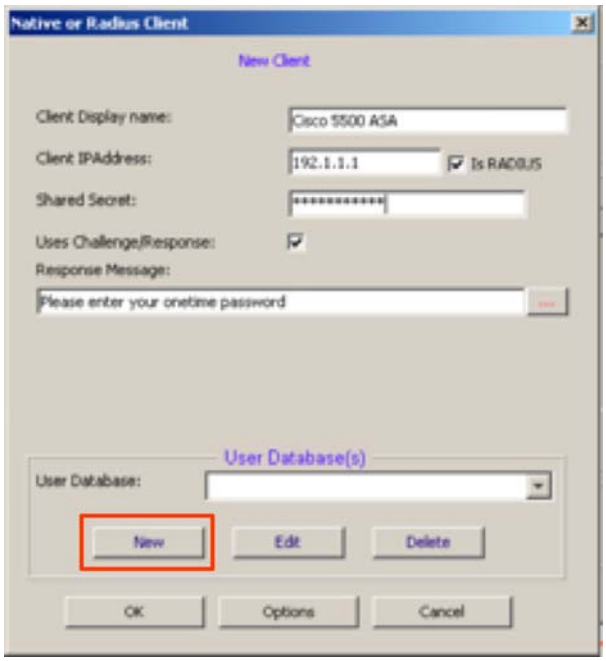
6.6 Add client

Click on Add Client and enter Client Display name and the ip-address for the Cisco 5500 ASA. Please note that you should not use the hostname here.

Make sure that “Is RADIUS” is checked and enter the correct Shared Secret.



In the category User Database (s) click New.

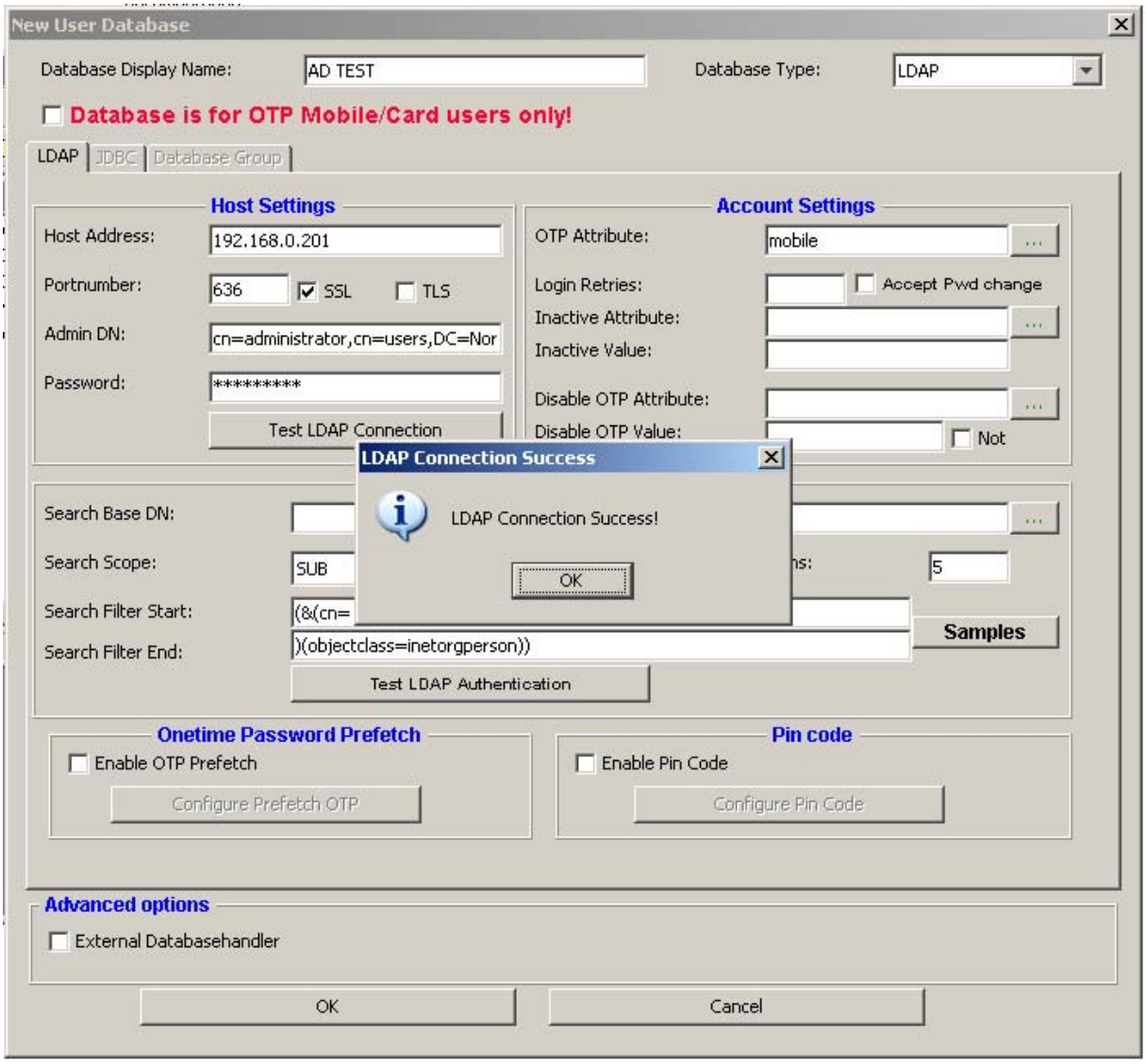


6.7 Configure LDAP

Enter a Database Display Name and the host address for your LDAP user database. In this case we are using Microsoft Active Directory with SSL and the users' mobile attribute for sending one time passwords.

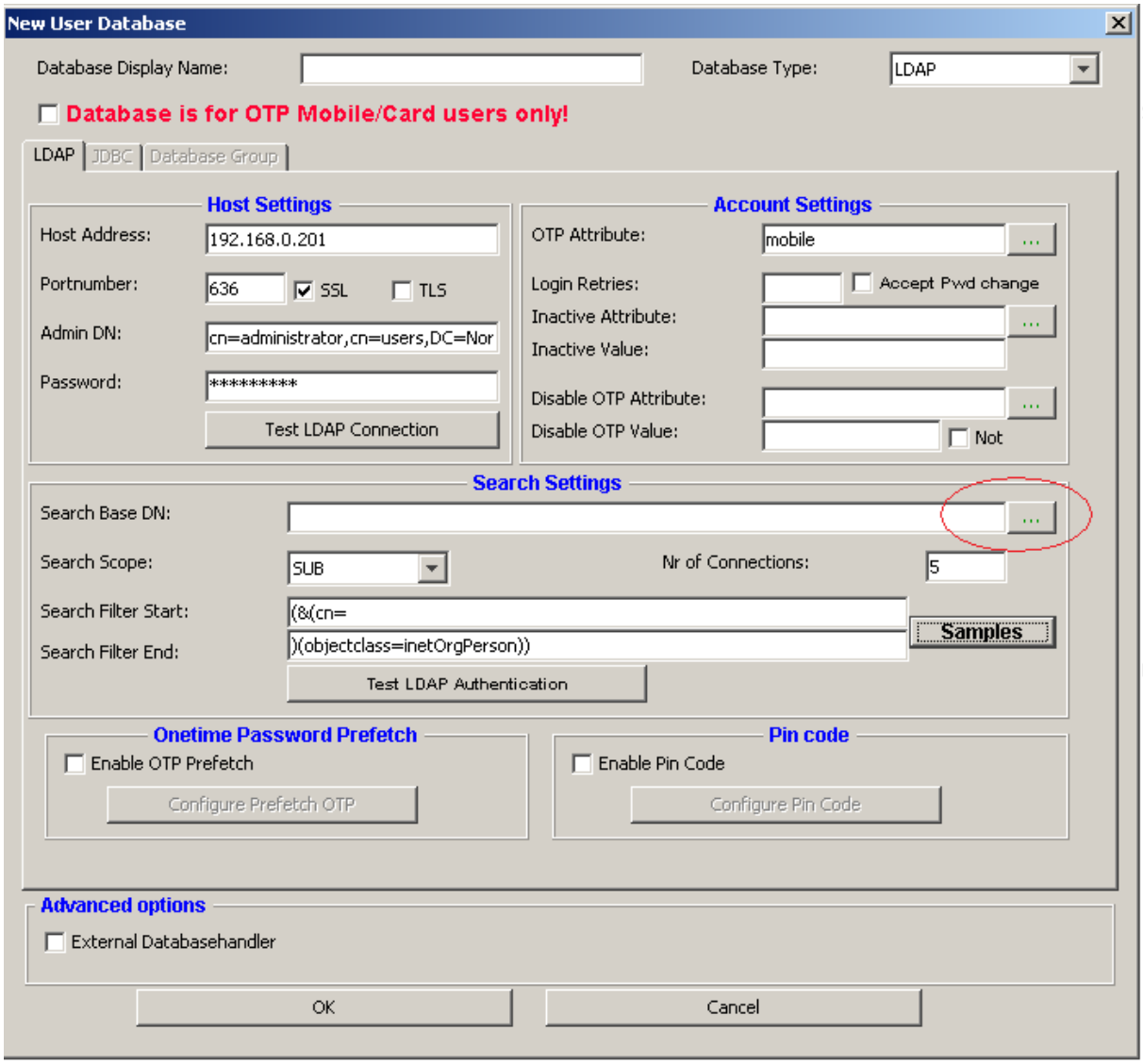
6.7.1 Test LDAP Connection

Click on Test LDAP Connection and make sure that you get an LDAP Connection Success.

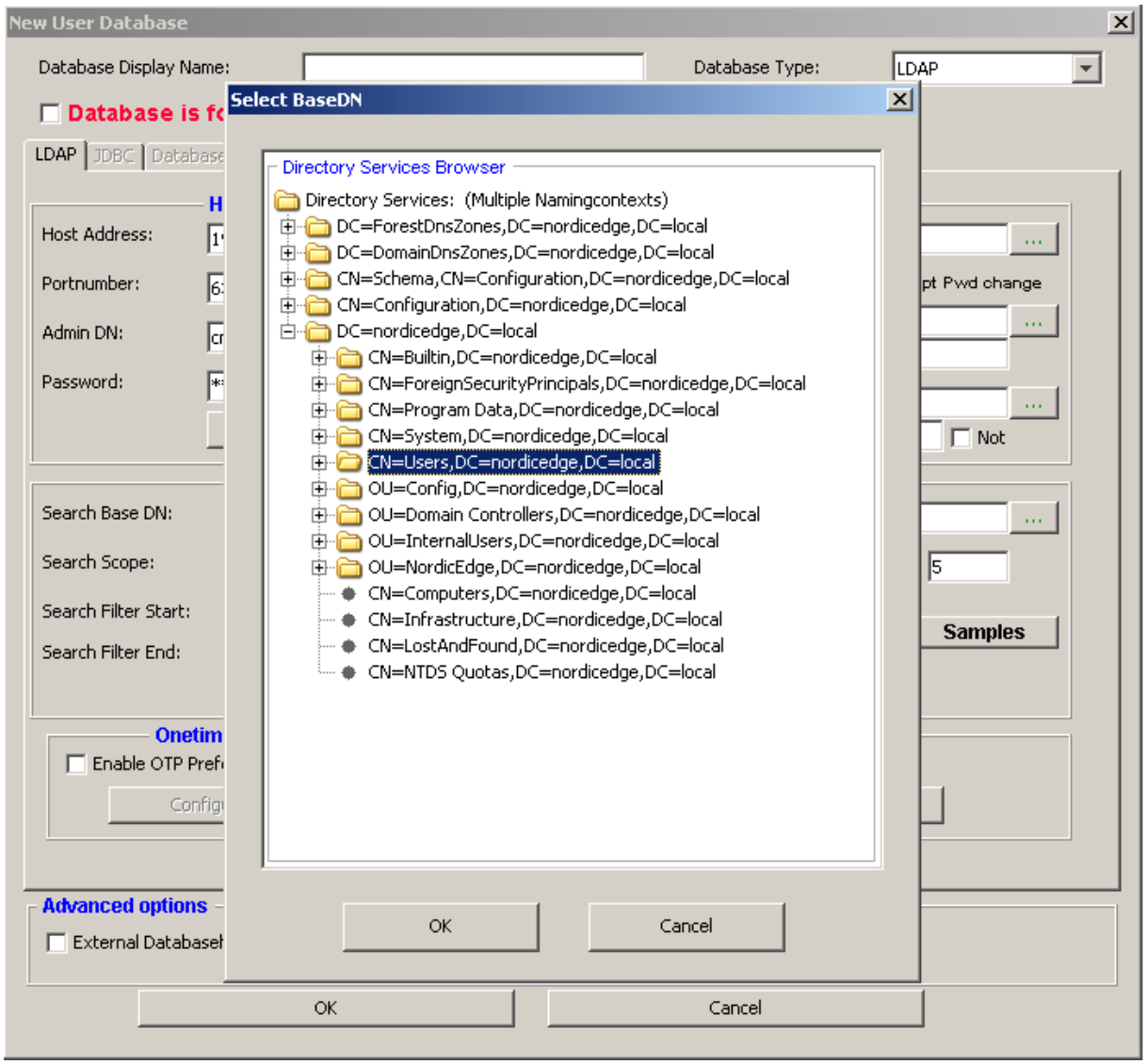


6.7.2 Selecting Search Base DN

Click on the box for selecting Search Base DN:

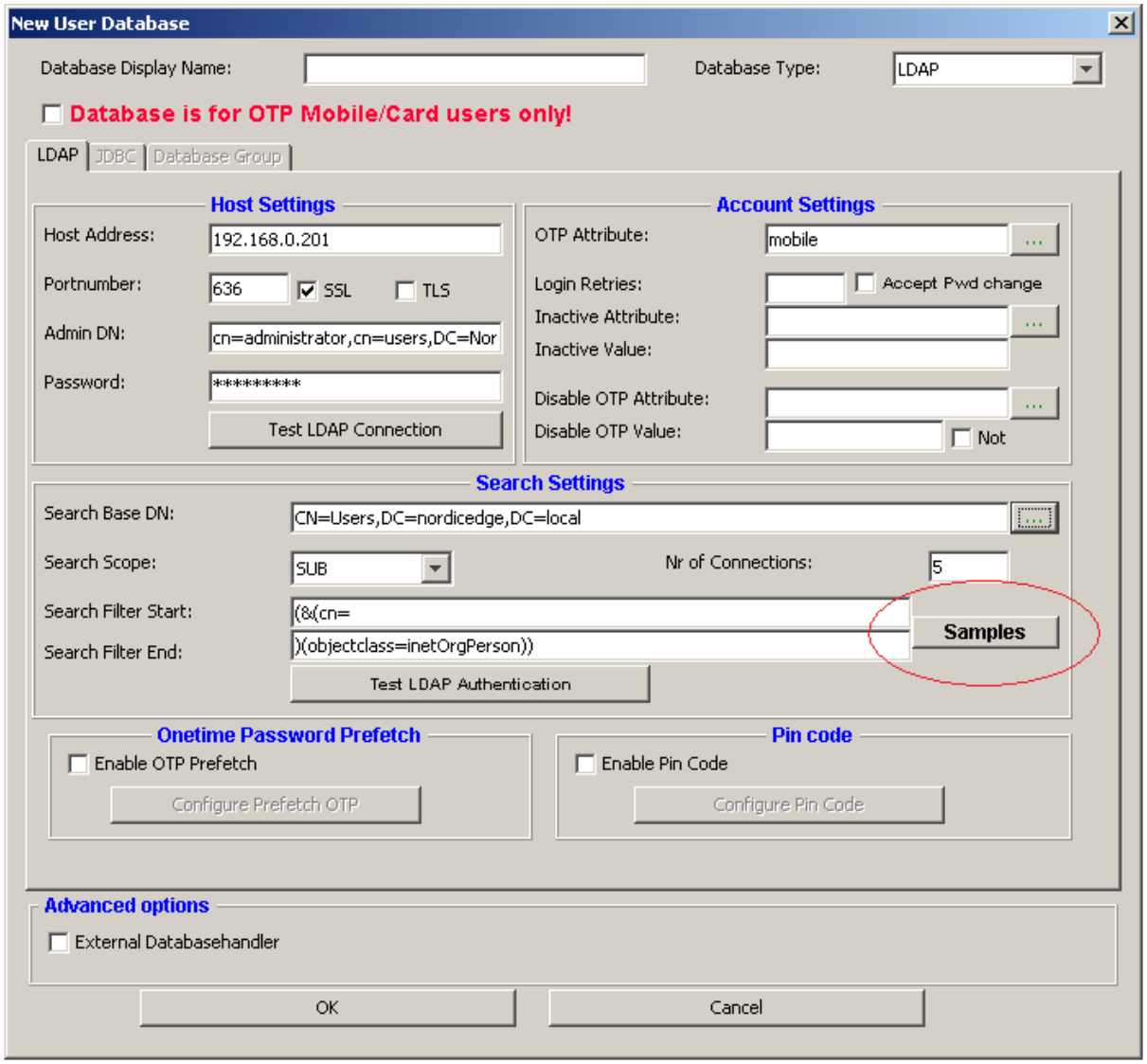


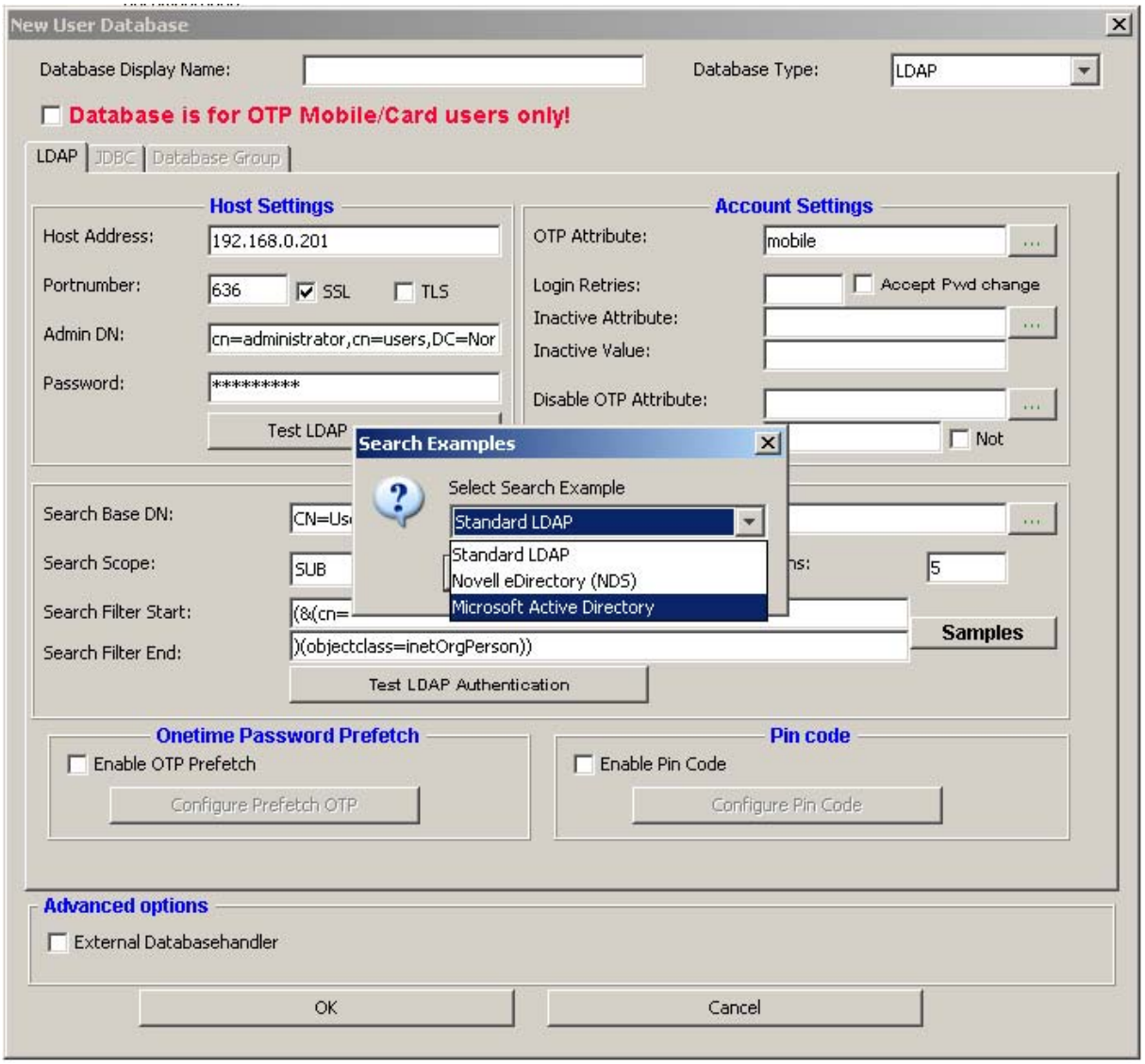
Select a Base Dn where your users are.

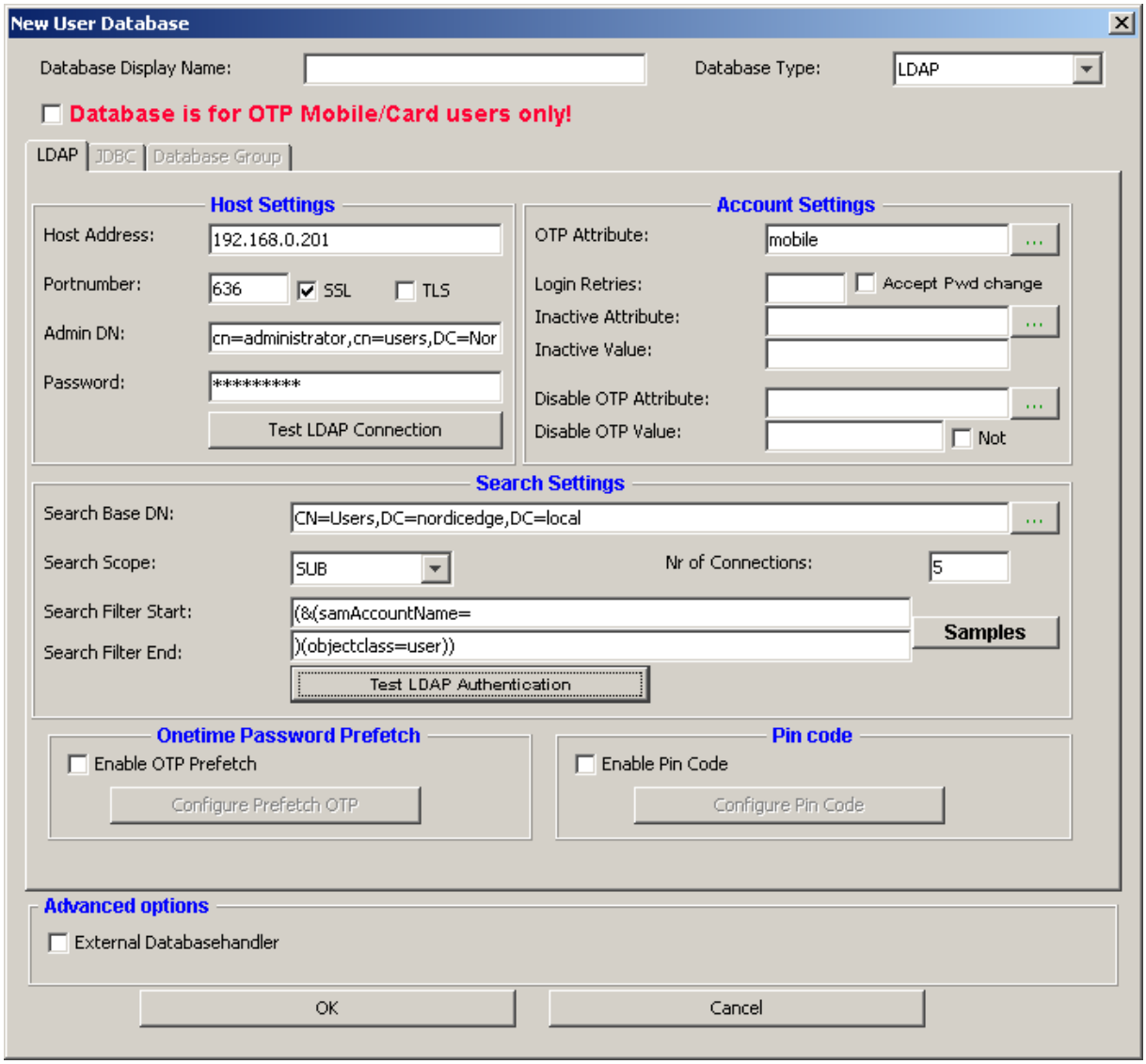


6.7.3 Select Search filter

Click on samples and select the right filter for your LDAP User database, in this case Active Directory.

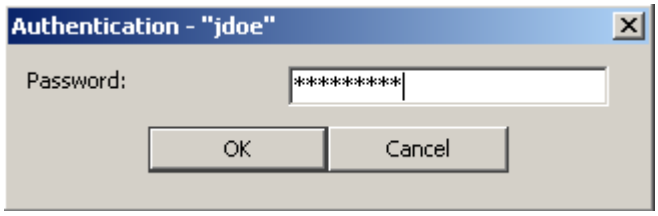


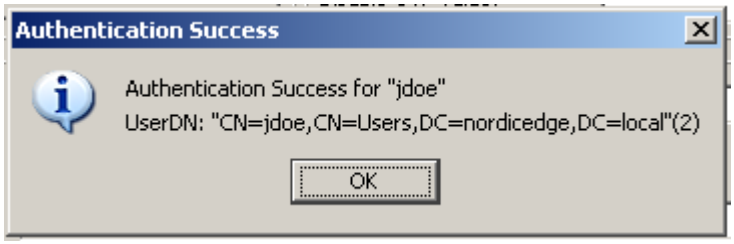




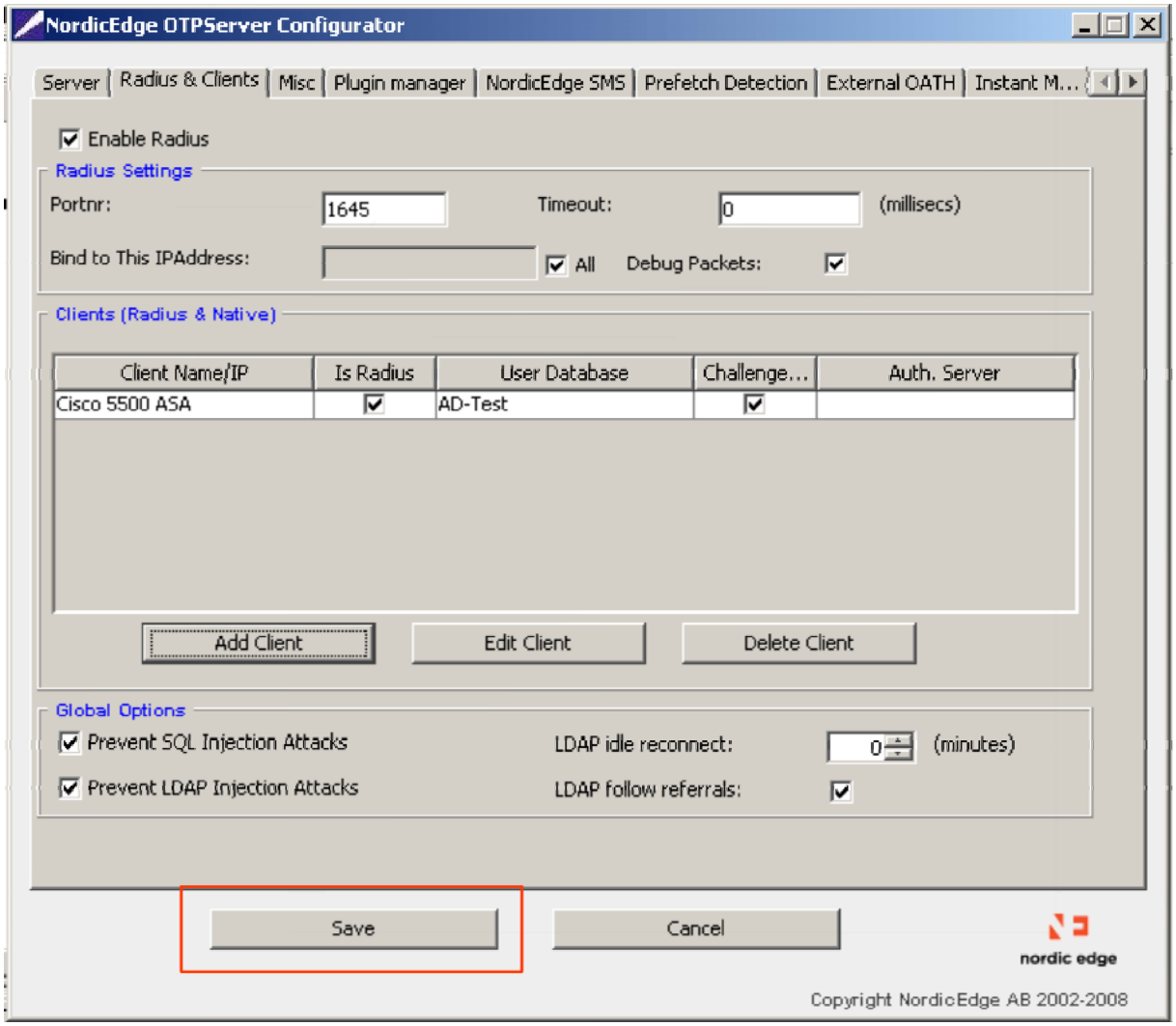
6.7.4 Test LDAP Authentication

Click on Test LDAP Authentication and make sure you can authenticate.





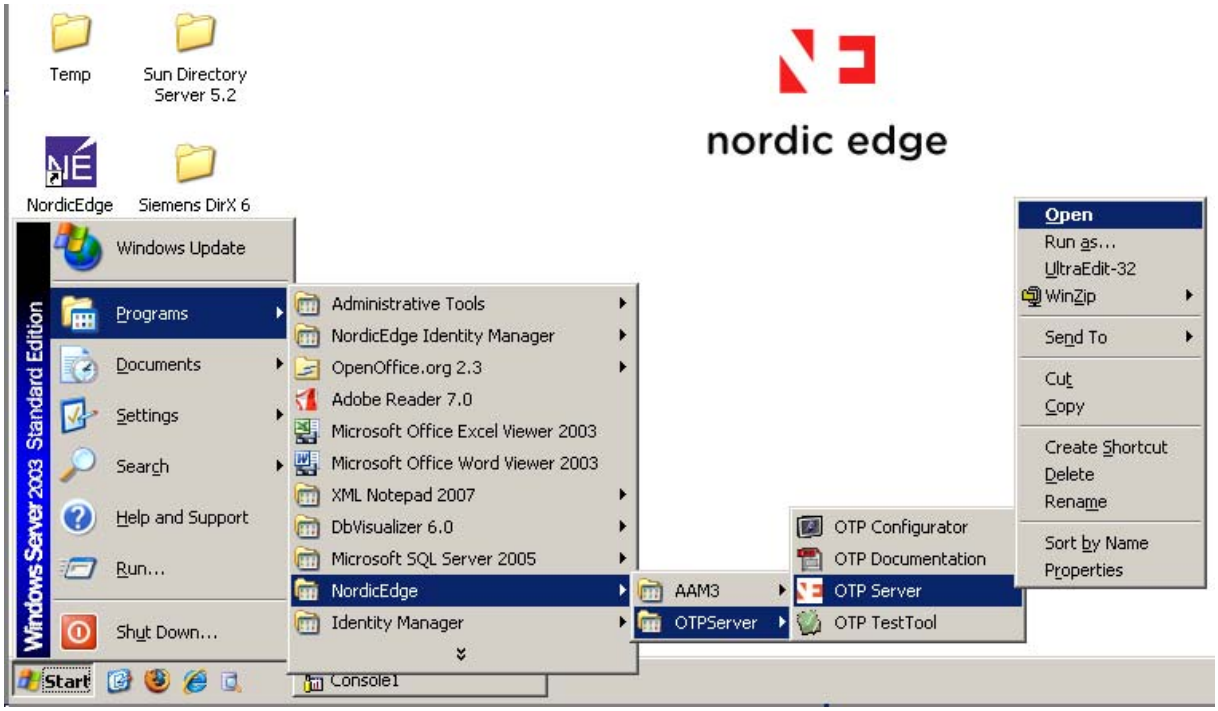
Exit the configurator by clicking OK twice and make sure to click on the Save button



End of Step “Configuring the One Time Password Server”

7 Start the One Time Password Server

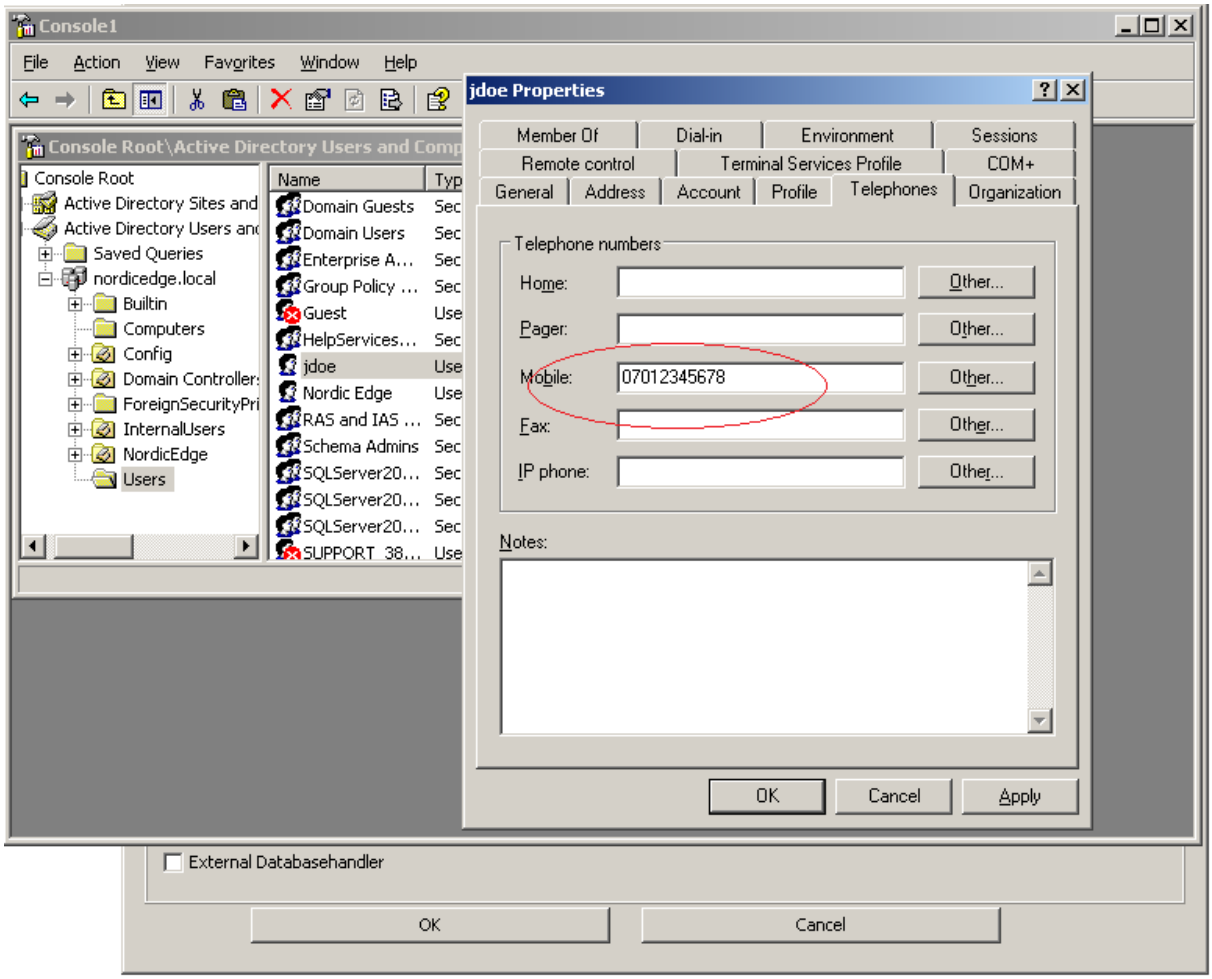
Start the One Time Password by going to Program folder, NordicEdge,OTPServer and klick on OTP Server



8 Add mobile phone number with Microsoft Management Console

Add mobile phone number to your test users mobile phone attribute

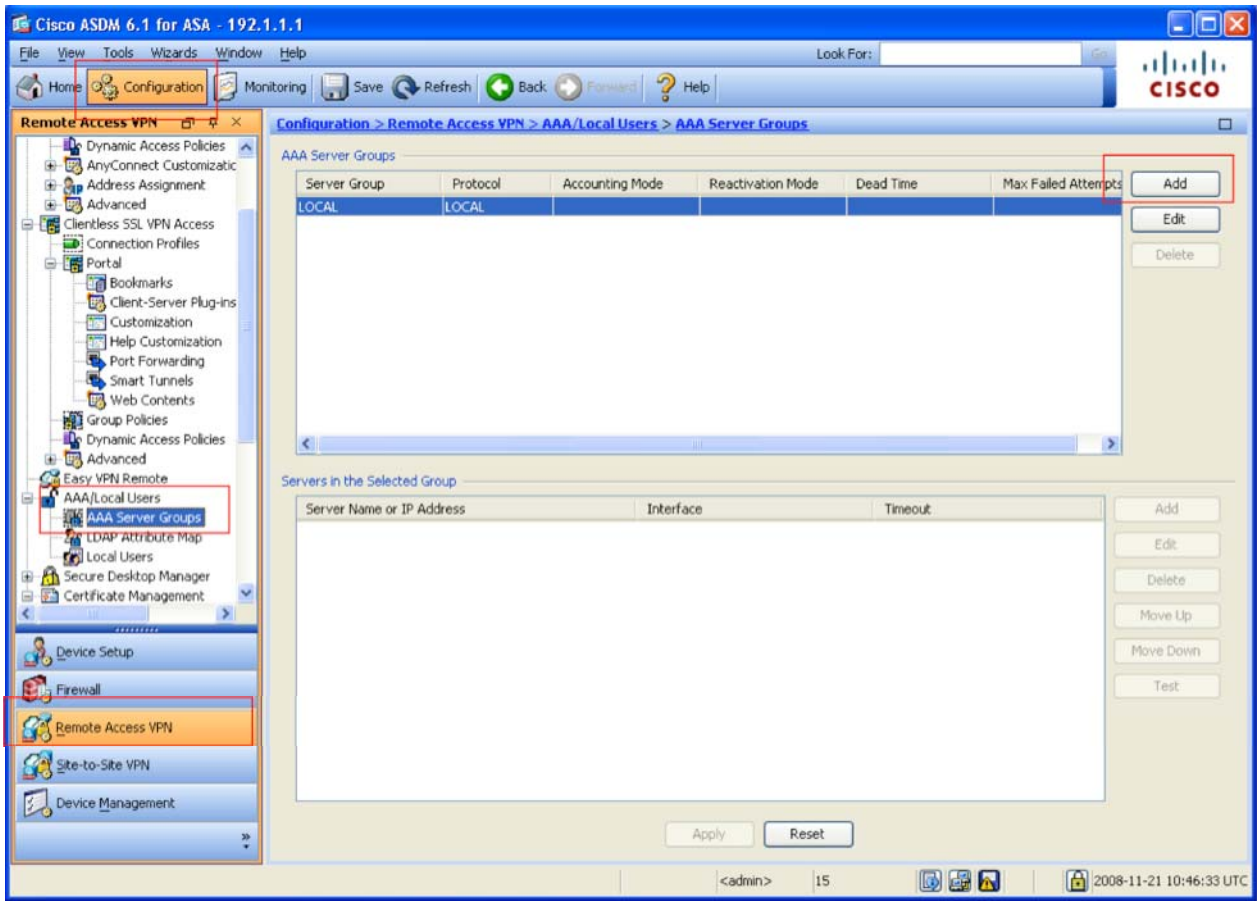
Start MMC and select the user that you want to use for testing and enter the mobile phone number in the Mobile attribute.



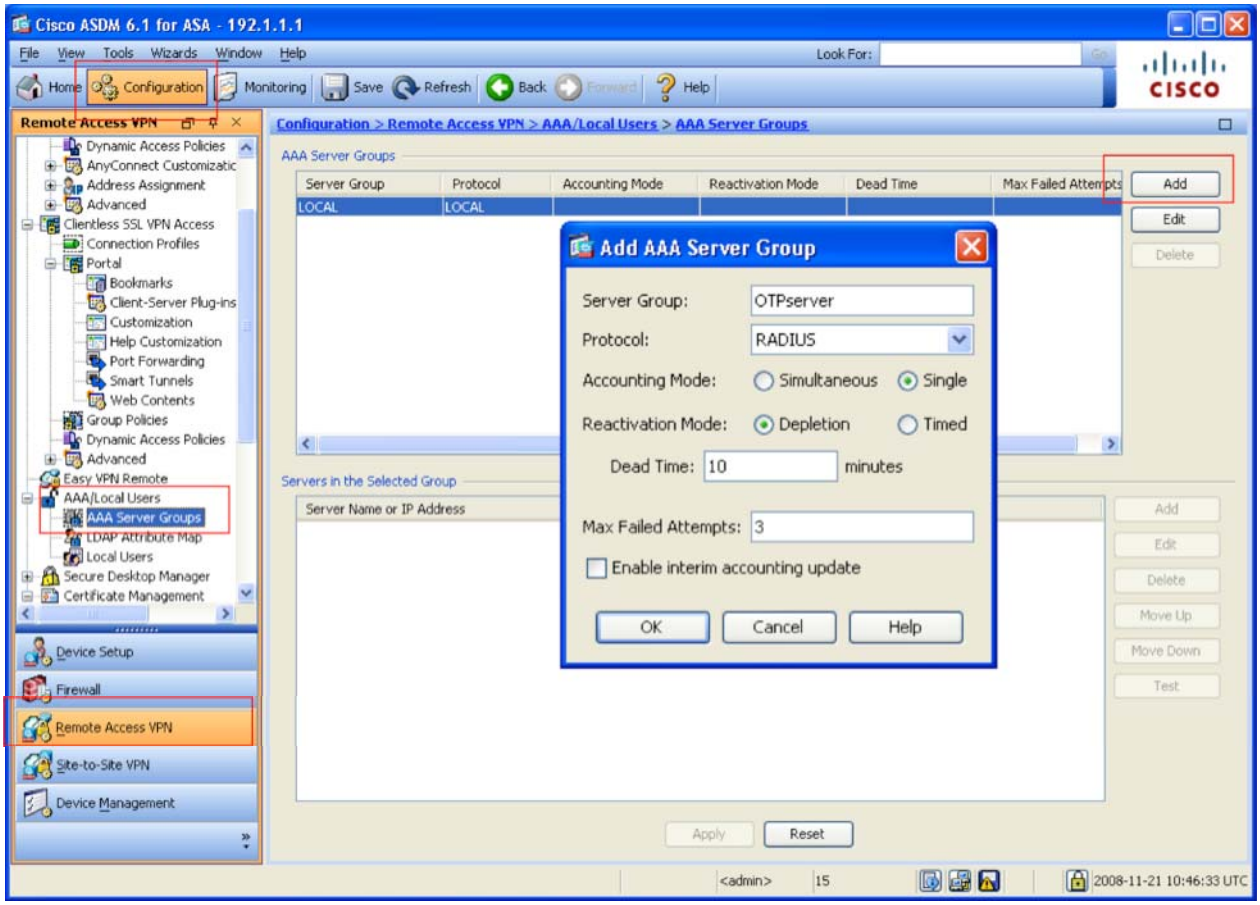
9 Configuring ASA5500 for SSL VPN authentication with Nordic Edge One Time Password Server

9.1 Start ASA device manager

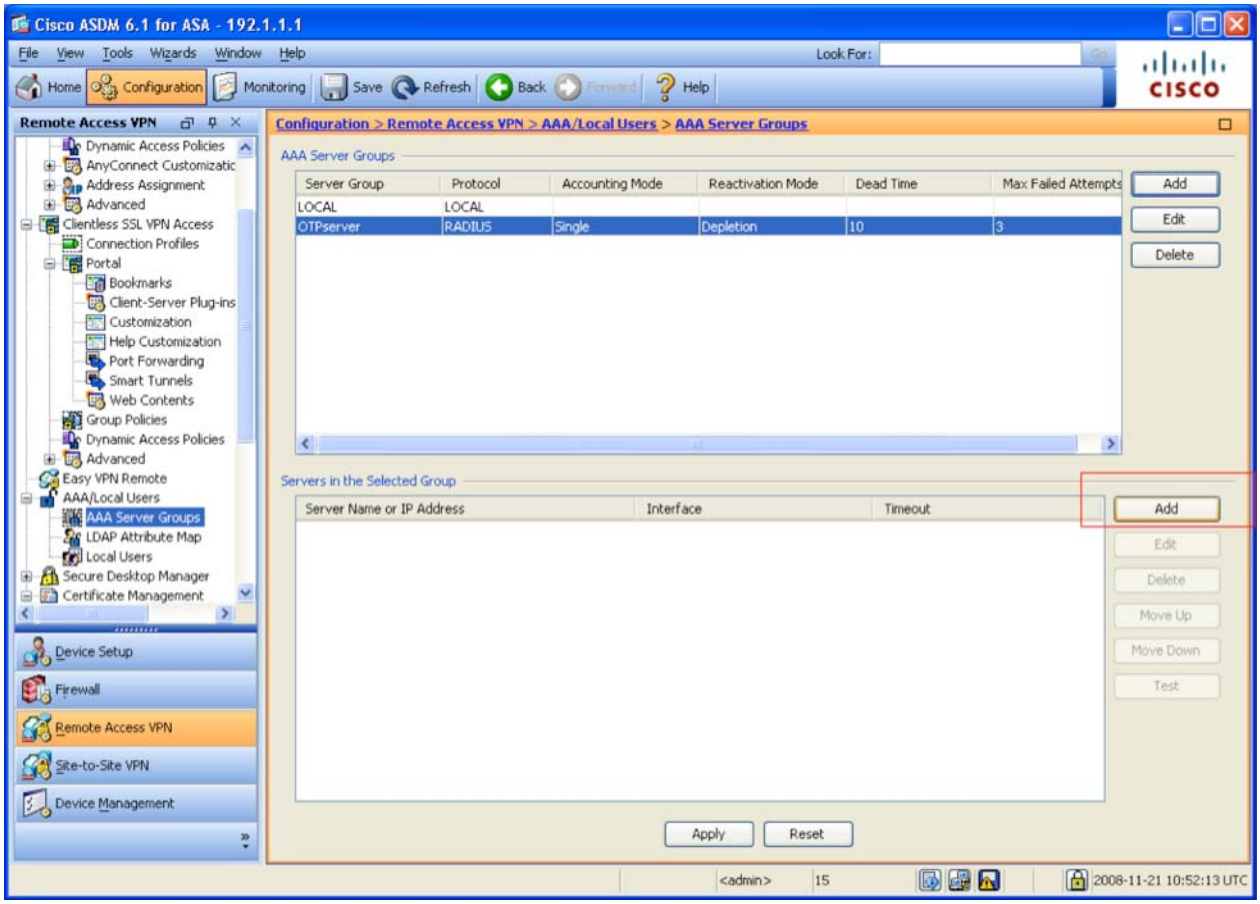
9.2 Browse to Configuration, Remote Access VPN, AAA/Local Users, AAA Server Groups and click Add.



9.3 Name Server Group OTPserver, choose protocol RADIUS

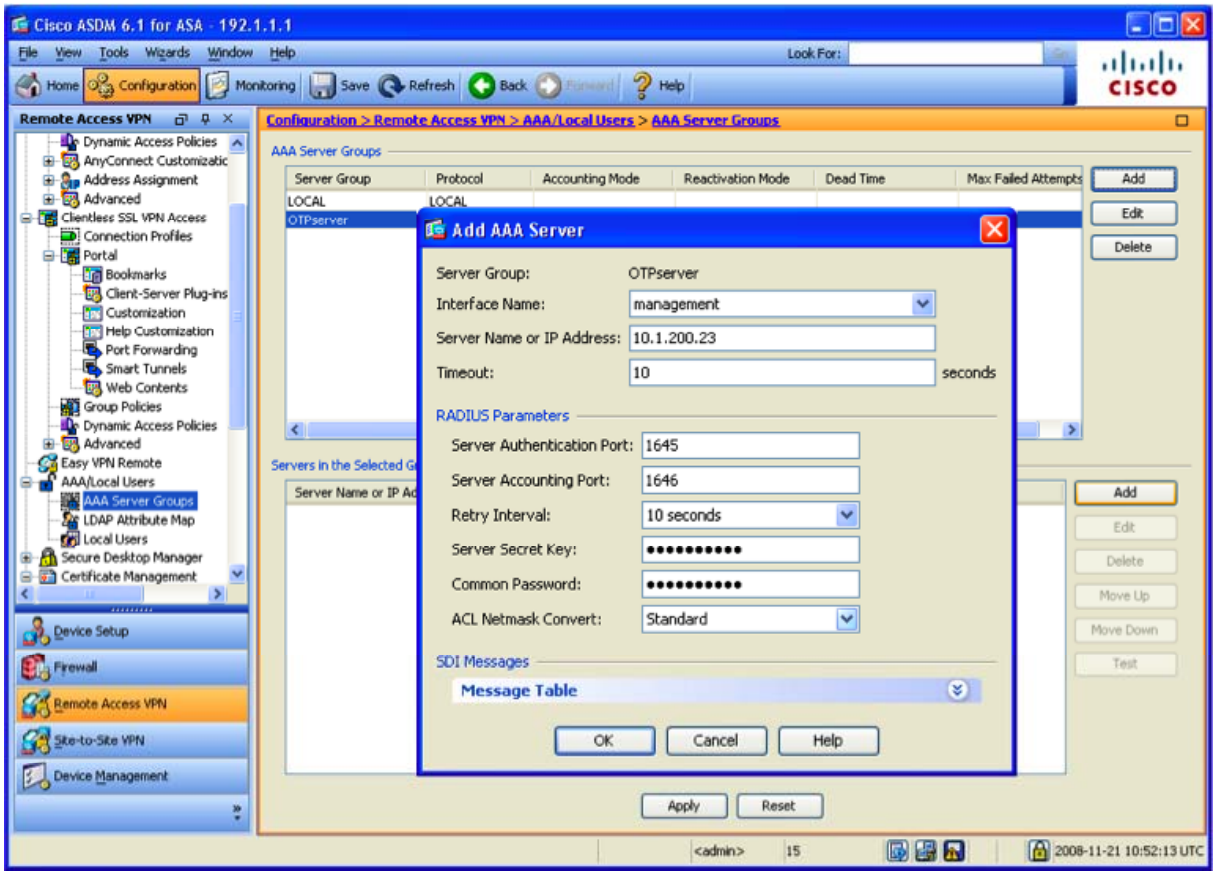


9.4 Add new radius server to the RADIUS group



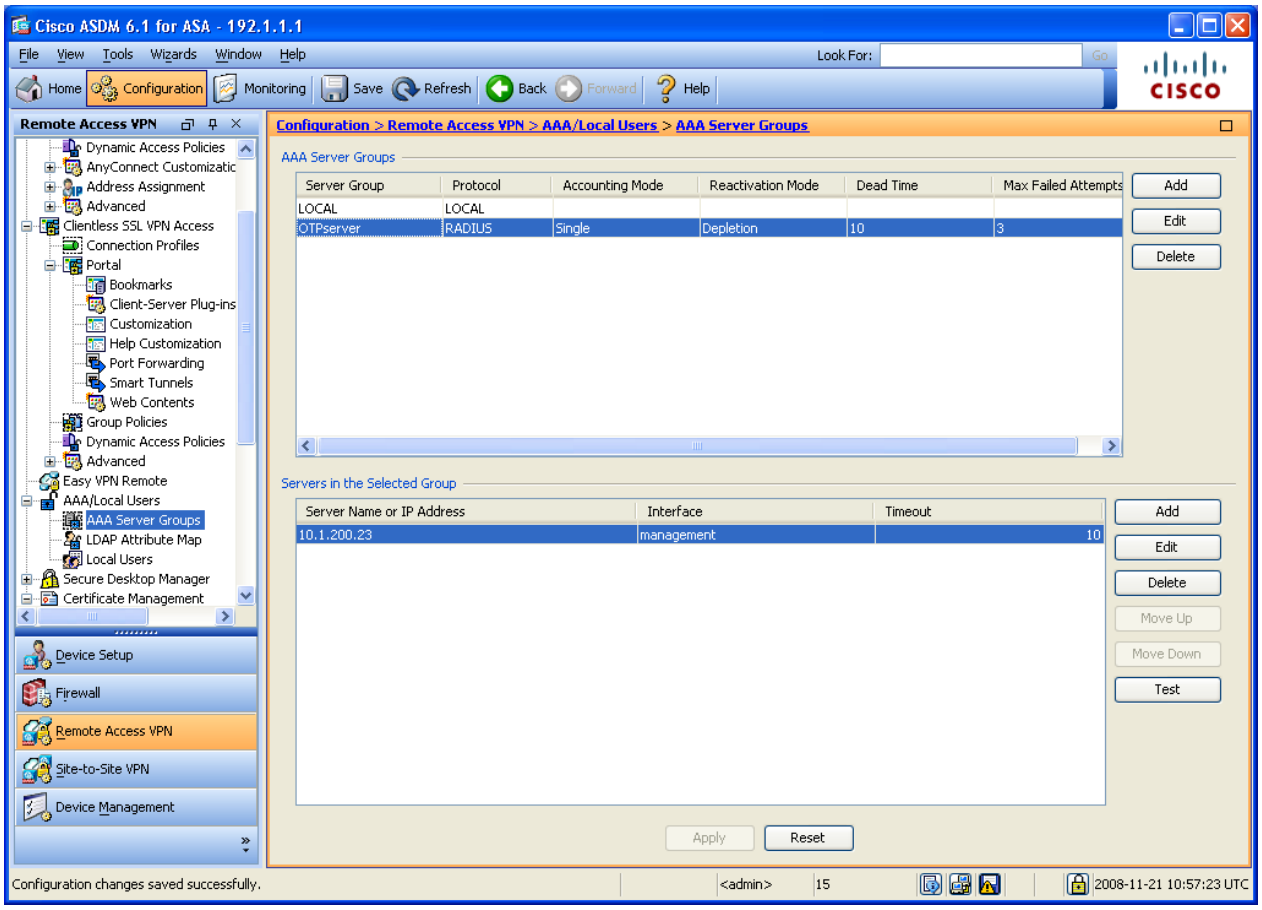
9.5 Configure Radius Server : Interface name, IP address to OTPserver and the pre-shared key between the One Time Password server and Cisco ASA5500.

Ensure you use the same radius ports in both OTPserver ASA5500.



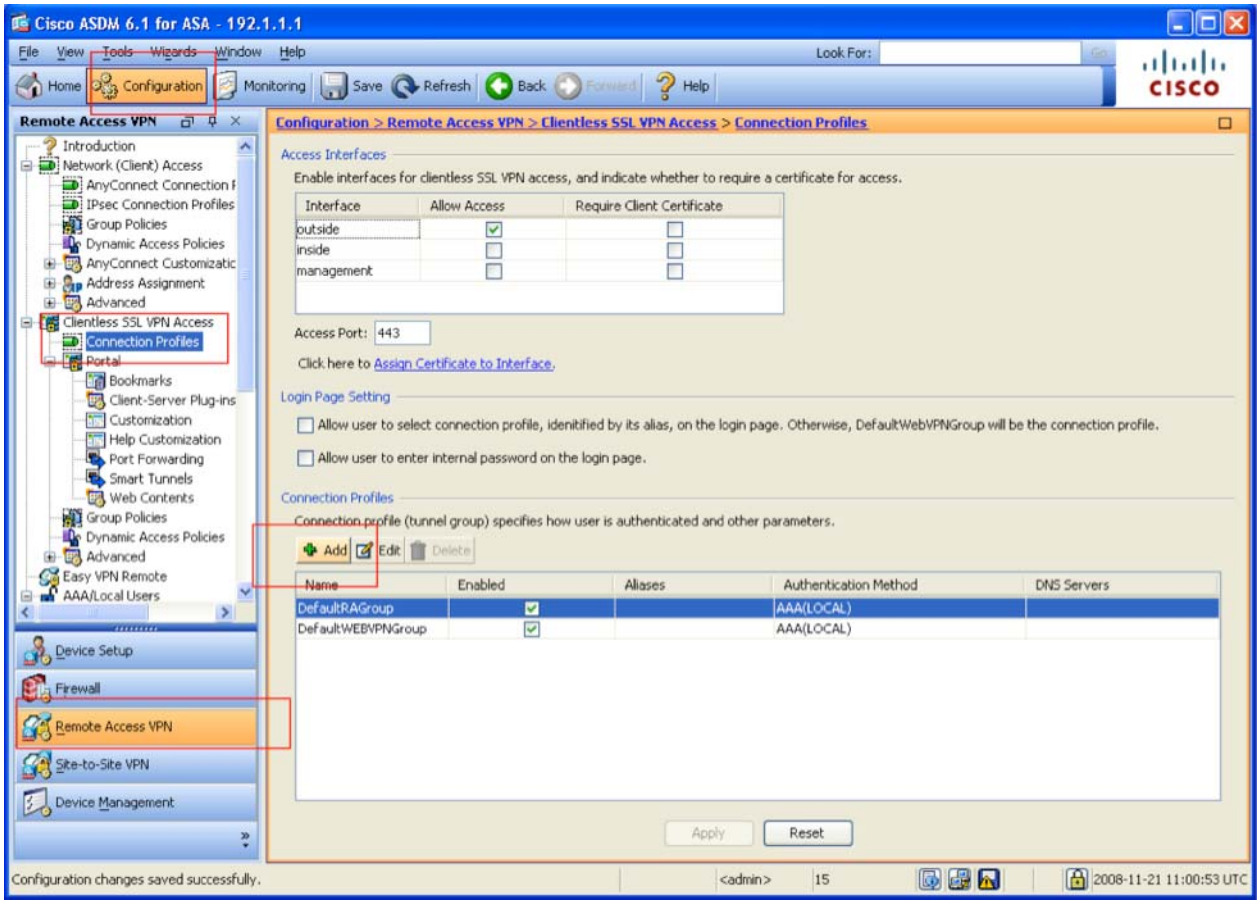
You have now configured a group ”OTPserver” and defined a Radius Server in this group.

This group can now be used as an authentication method.



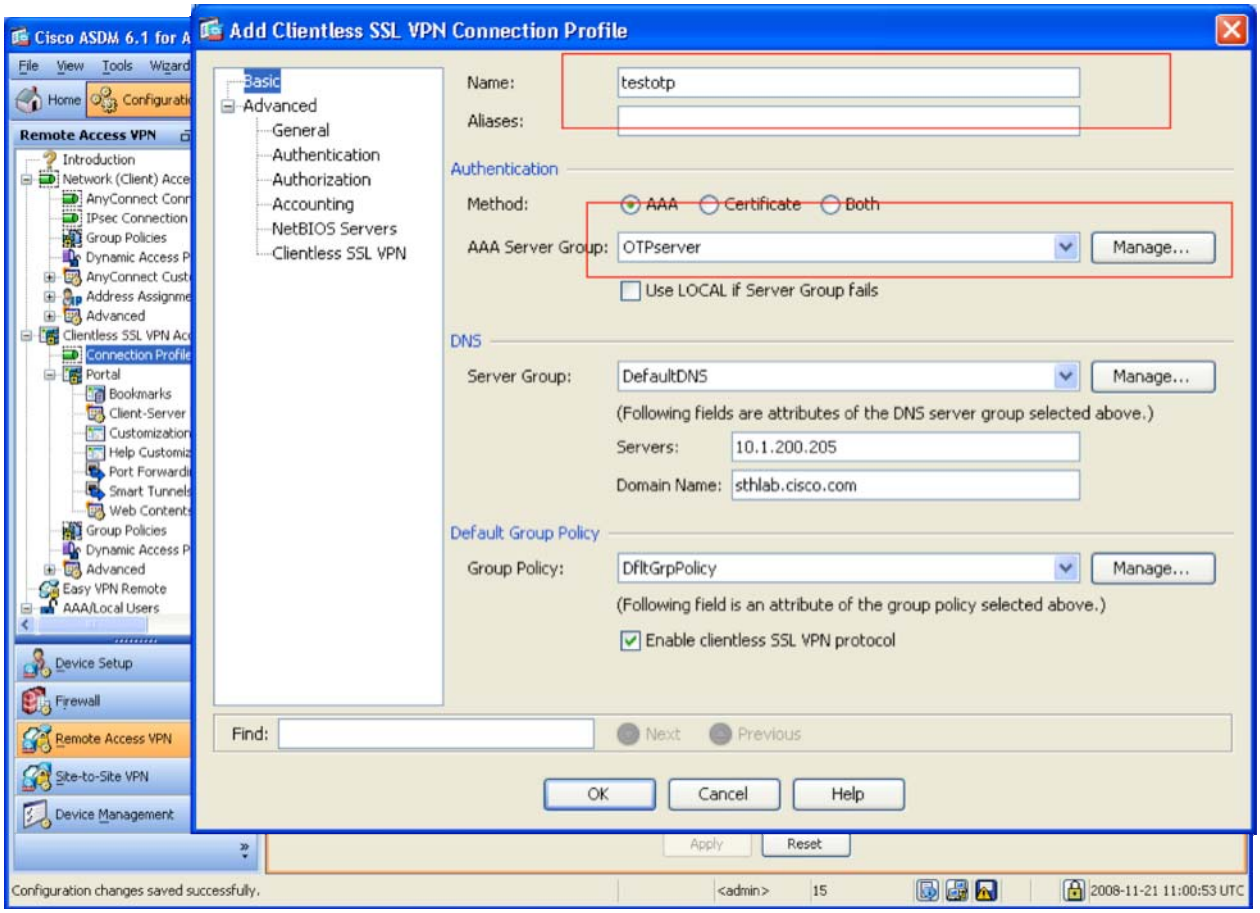
9.6 Create a ”test” connection profile (in case you want to test this for certain users only).

9.6.1 Browse to Configuration/Remote Access/Clientless SSL VPN Access/Connection Profiles and click Add



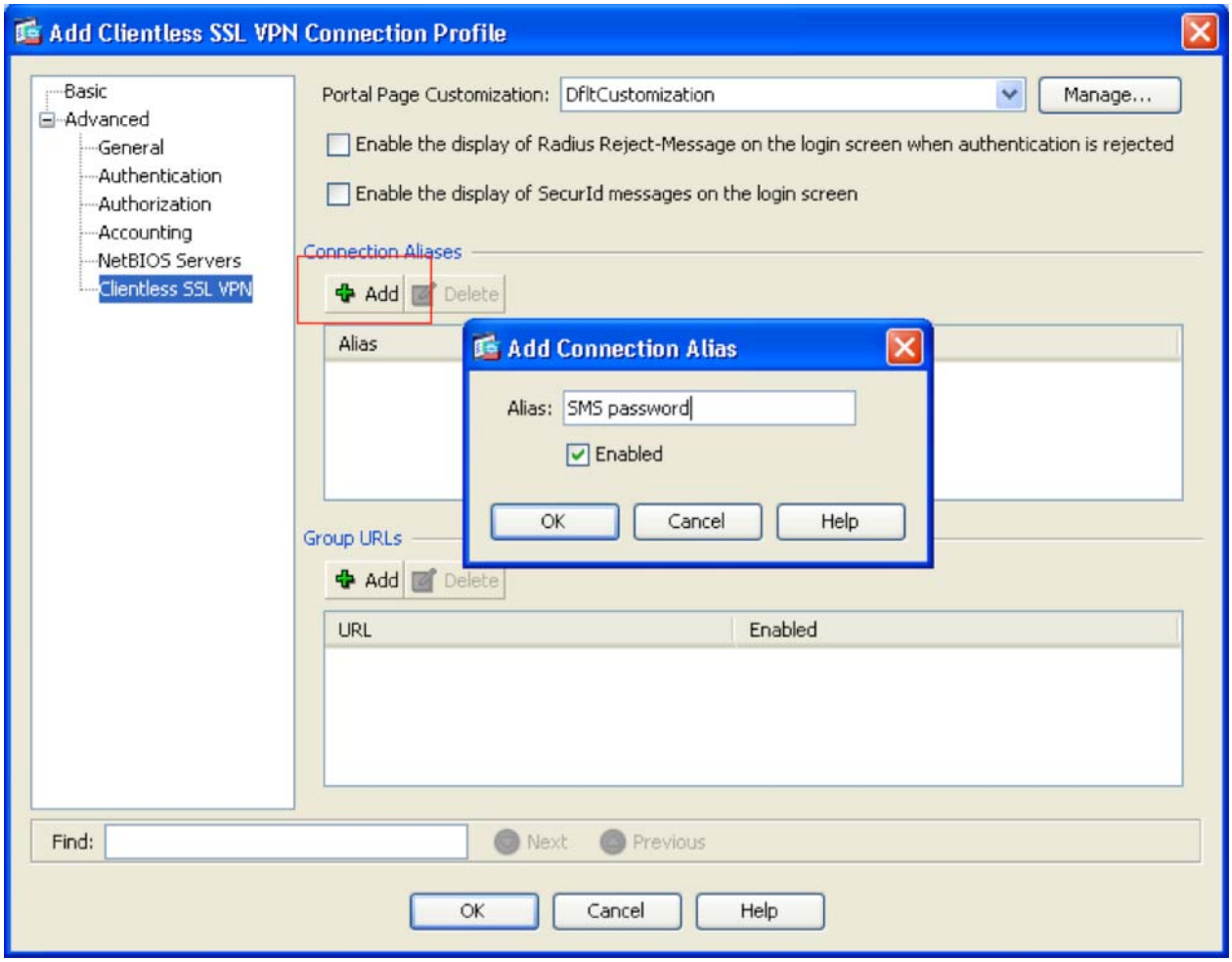
9.6.2 Specify Connection Profile Name

9.6.3 Specify AAA Server Group = OTPserver



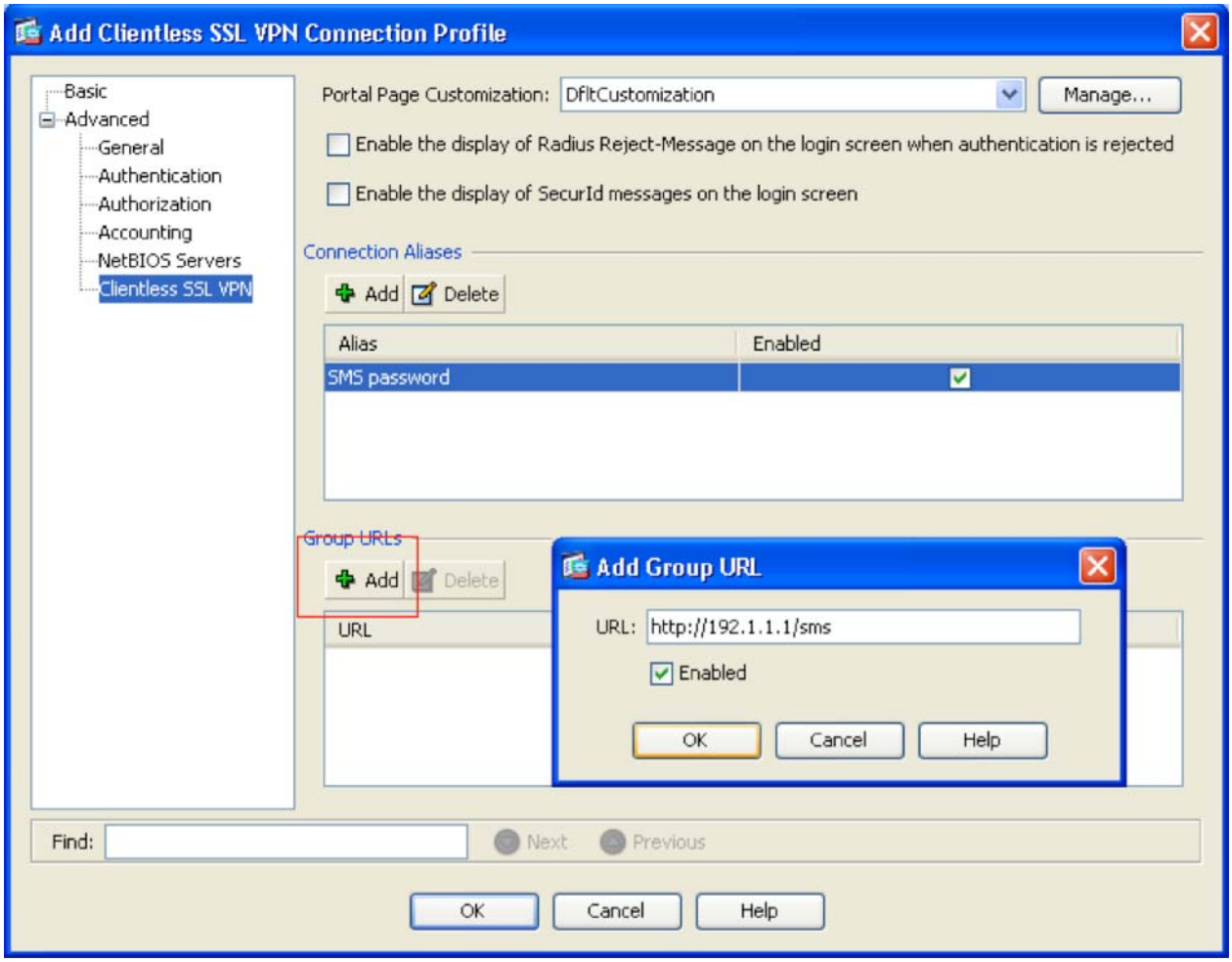
9.6.4 Edit Connection Profile Clientless SSL VPN Settings

9.6.5 Add Alias if user should be able to select authentication method by drop-down-list



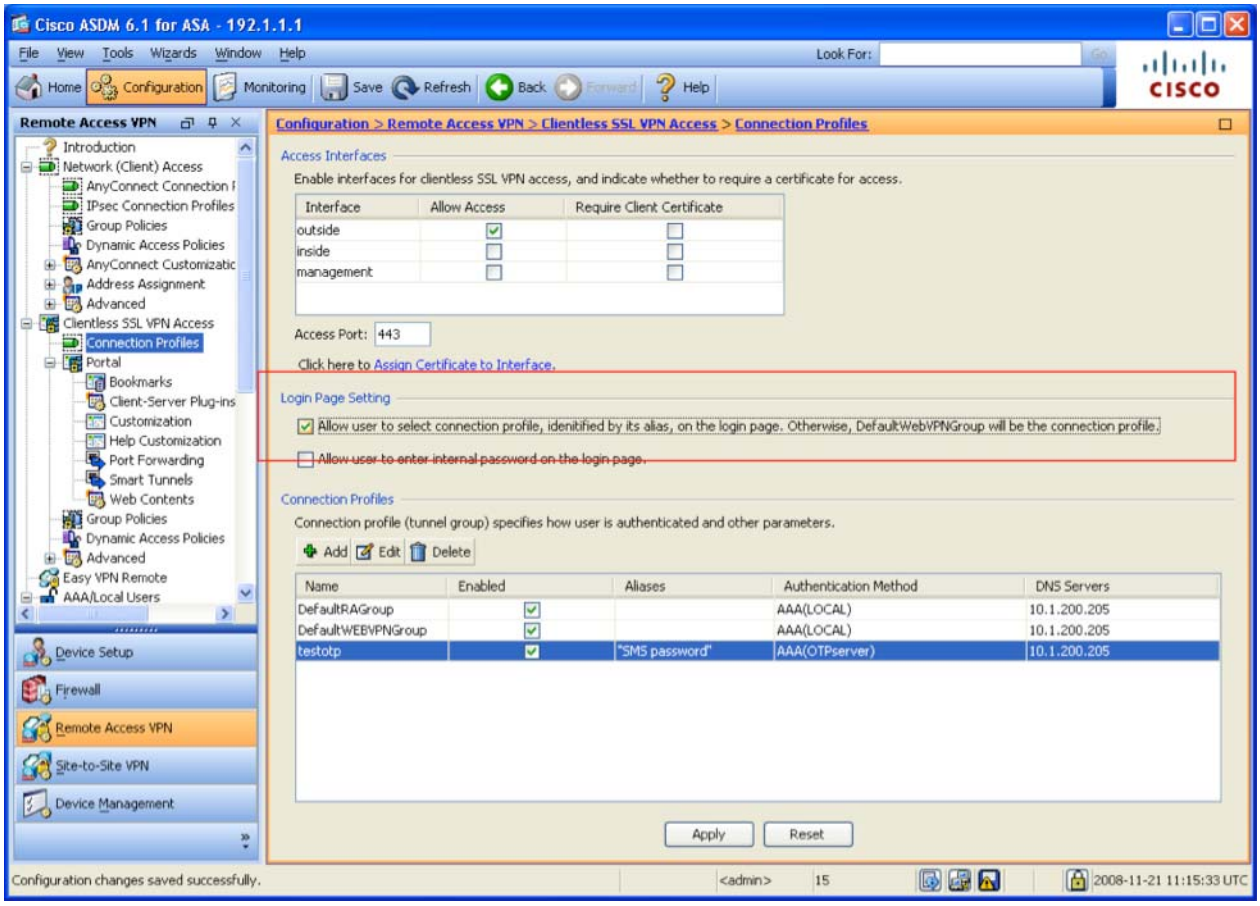
9.6.6 Edit Connection Profile Clientless SSL VPN Settings

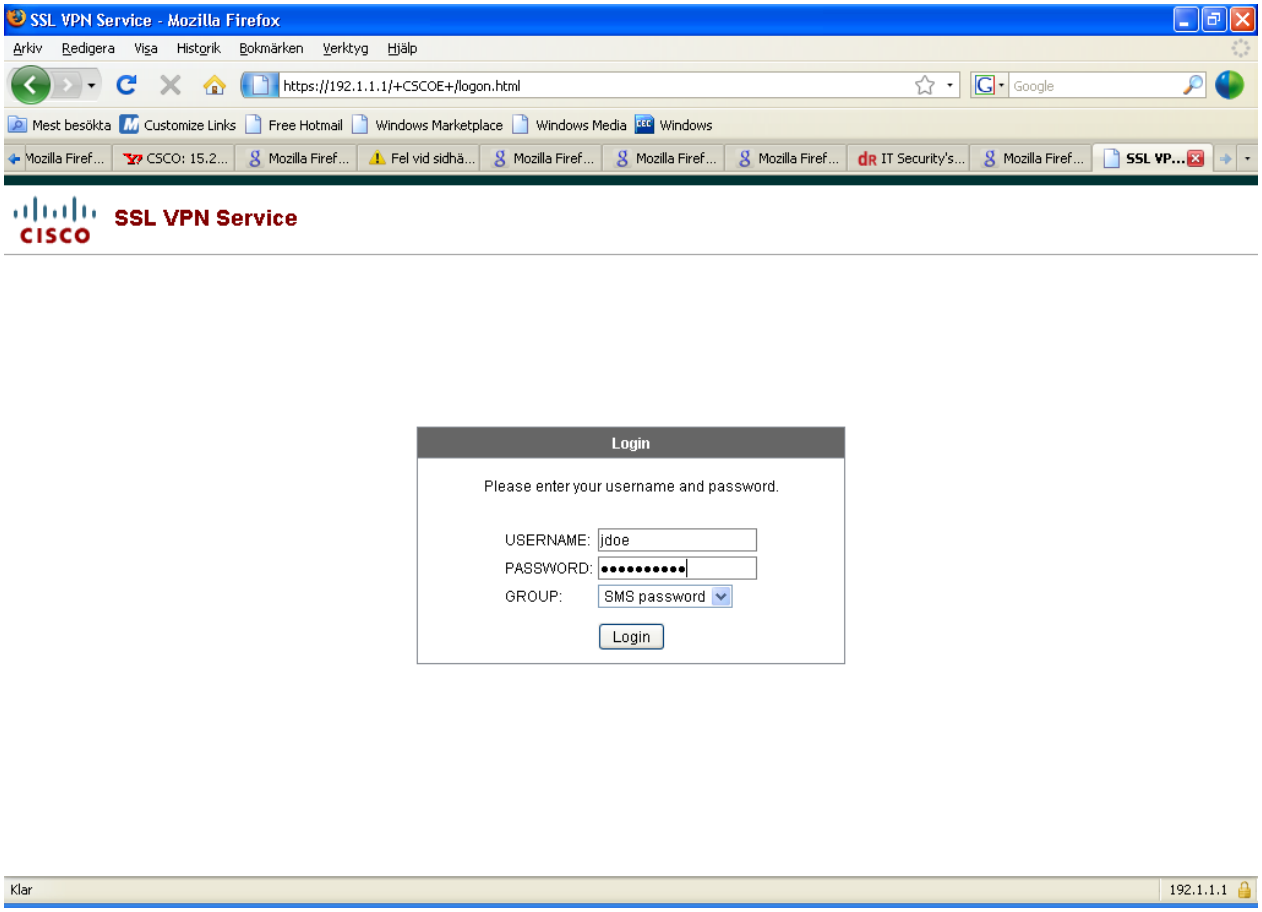
9.6.7 Add Group URL if user should be able to select authentication by specifying URL



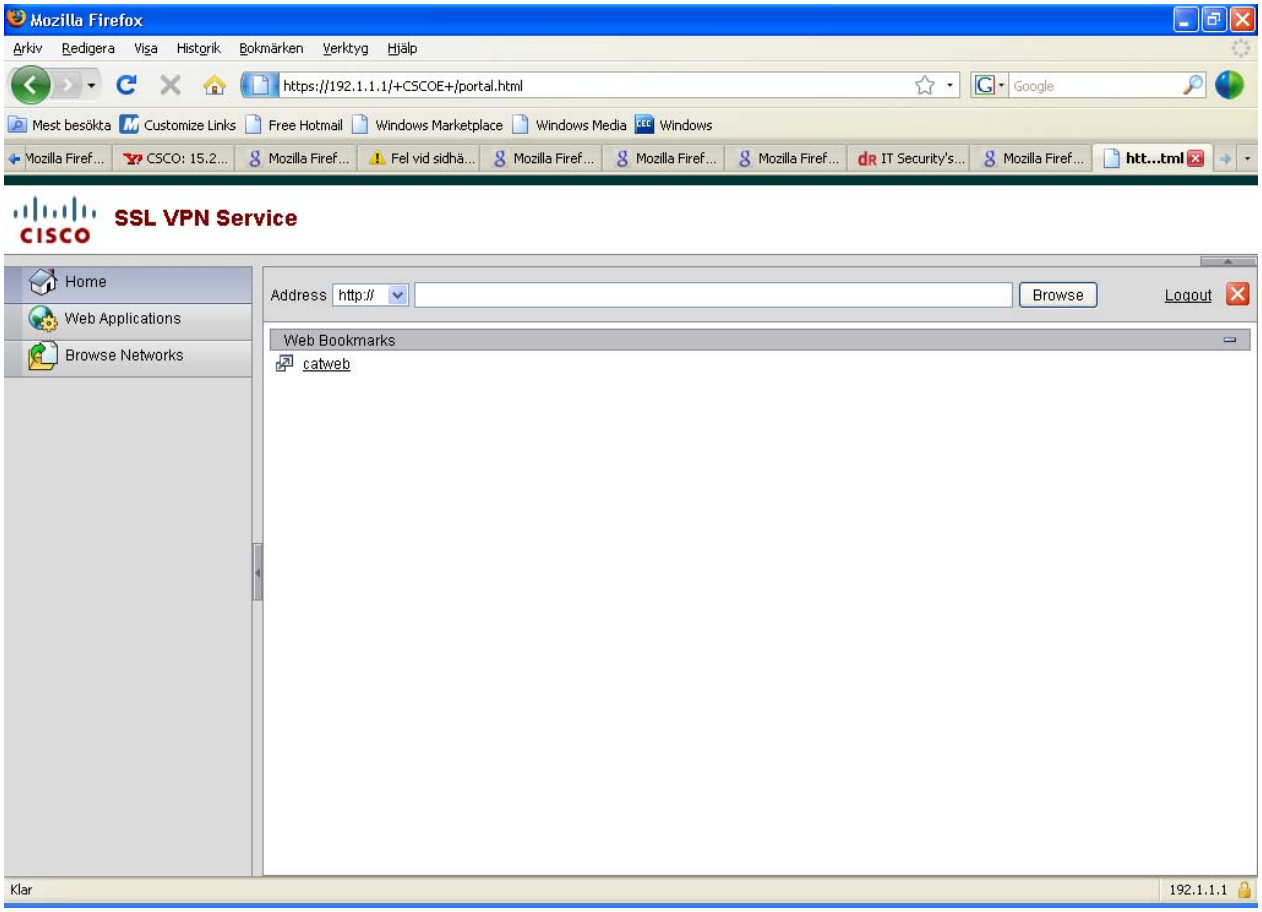
9.6.8 If user should be allowed to select authentication method by drop-down-list,

9.6.9 select this item.



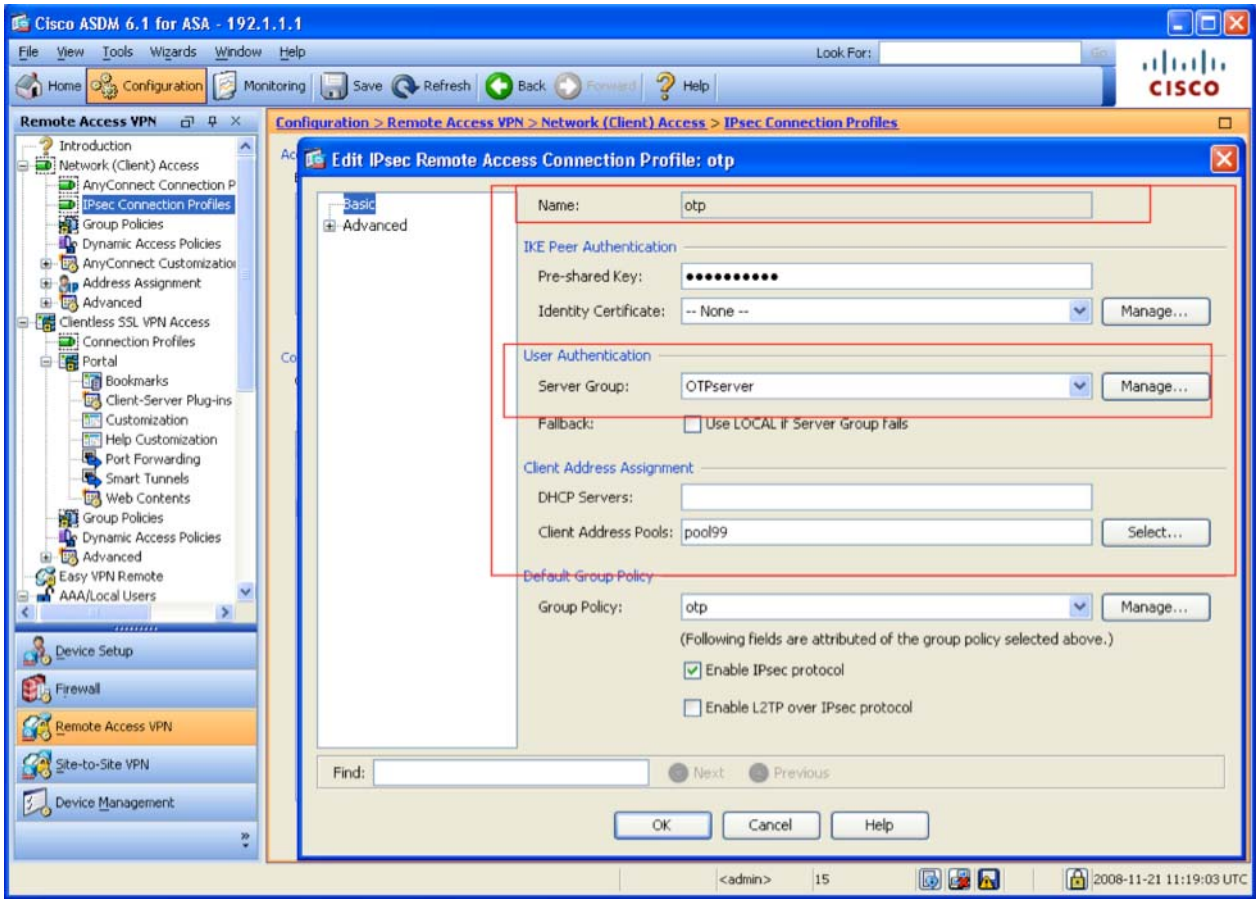


Login successful, the user will now get to his portal, which can be customized depending on Active Directory membership, PC health status (antivirus , hotfix etc) and authentication method



10 Configuring ASA5500 for Cisco VPN Client authentication with Nordic Edge OTP Server

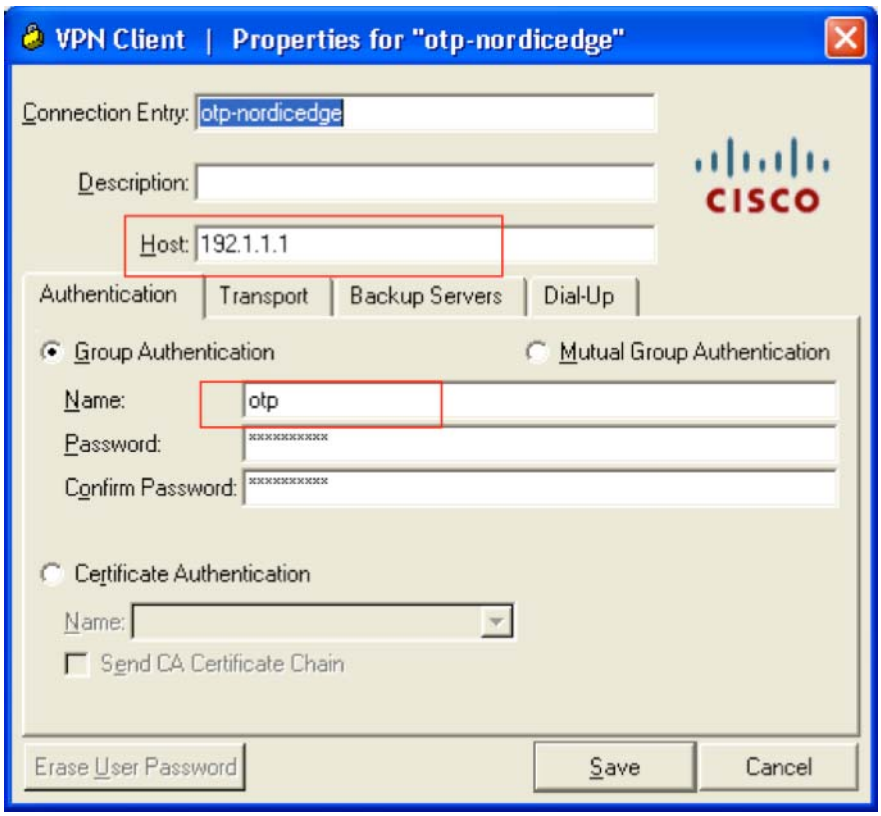
10.1 Add a new (or Edit an existing) Cisco VPN Client Connection Profile to use the OTPserver



10.2 At the Cisco VPN Client, create an entry with correct name and password

- **Name must match the connection profile name at previous slide.**
- **Password must match the pre-shared key in ASA5500.**

(Note : This can be distributed via MSI installation)



11 Start testing

11.1 Enter your Userid and password as usual

11.2 You will receive a one-time password to your mobile phone within a couple of seconds.

11.3 Enter your one time password and click on “OK”.

12 Purchase

If you want to purchase the product, you are more than welcome to contact us at sales@nordicedge.se and we will send you an offer. Please note that the price will depend on number of users.

13 Technical questions

If you have any technical questions, please contact us at support@nordicedge.se ---

Thank you for showing interest in our product

The Nordic Edge One Time Password Server Team